

Privacy Act Issuances: 2009

[\[BACK TO LIST OF AGENCIES\]](#)

Department of Justice

Table of Contents

[Systems of Records Published in the *Federal Register* Between January 2, 2008 and December 31, 2009](#)

[Statement of Routine Uses for All Systems of Records](#)

[JUSTICE-001, Accounting Systems for the Department of Justice.](#)

[JUSTICE-002, DOJ Computer Systems Activity and Access Records.](#)

[JUSTICE-003, Correspondence Management Systems \(CMS\) for the Department of Justice.](#)

[JUSTICE-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Requests and Administrative Appeals for the Department of Justice.](#)

[JUSTICE-005, Nationwide Joint Automated Booking System \(JABS\).](#)

[JUSTICE-006, Personnel Investigation and Security Clearance Records for the Department of Justice.](#)

[JUSTICE-007, Reasonable Accommodations for the Department of Justice \(DOJ\).](#)

[JUSTICE-008, Department of Justice Grievance Records.](#)

[JUSTICE-009, Emergency Contact systems for the Department of Justice.](#)

[JUSTICE-010, Leave Sharing Systems.](#)

[JUSTICE-011, Access Control System \(ACS\).](#)

[JUSTICE-012, Department of Justice Regional Data Exchange System \(RDEX\).](#)

[DOJ-013, Justice Federal Docket Management System \(Justice FDMS\).](#)

[DOJ-014, Employee Directory Systems for the Department of Justice](#)

Bureau of Alcohol Tobacco, Firearms, and Explosives

[JUSTICE/ATF-001—Administrative Record System](#)

[JUSTICE/ATF-003—Criminal Investigation Report System](#)

[JUSTICE/ATF-006—Internal Security Record System](#)

[JUSTICE/ATF-007—Personnel Record System](#)

[JUSTICE/ATF-008—Regulatory Enforcement Record System](#)

[JUSTICE/ATF-009—Technical and Scientific Services Record System](#)

[JUSTICE/ATF-010—Training and Professional Development Record System](#)

Antitrust Division

[JUSTICE/ATR-001, Antitrust Division Expert Witness File.](#)

[JUSTICE/ATR-003, Index of Defendants in Pending and Terminated Antitrust Cases.](#)

[JUSTICE/ATR-004, Statement by Antitrust Division Officials \(ATD Speech File\).](#)

[JUSTICE/ATR-005, Antitrust Caseload Evaluation System \(ACES\)—Time Reporter.](#)

[JUSTICE/ATR-006, Antitrust Caseload Evaluation System \(ACES\)—Monthly Report.](#)

[JUSTICE/ATR-007, Antitrust Division Case Cards.](#)

[JUSTICE/ATR-009, Public Complaints and Inquiries File.](#)

[JUSTICE/ATR-014, Civil Investigative Demand \(CID\) Tracking System.](#)

Board of Immigration Appeals

[JUSTICE/BIA-001, Decisions of the Board of Immigration Appeals.](#)

[JUSTICE/BIA-002, Roster of Organizations and their Accredited Representative Recognized by the Board of Immigration Appeals.](#)

Bureau of Prisons

[JUSTICE/BOP-001, Prison Security and Intelligence Record System.](#)

[JUSTICE/BOP-003, Industrial Inmate Employment Record System.](#)

[JUSTICE/BOP-004, Inmate Administrative Remedy Record System.](#)

[JUSTICE/BOP-005, Inmate Central Records System.](#)

[JUSTICE/BOP-006, Inmate Trust Fund Accounts and Commissary Record System.](#)

[JUSTICE/BOP-007, Inmate Physical and Mental Health Record System.](#)

[JUSTICE/BOP-008, Inmate Safety and Accident Compensation Record System.](#)

[JUSTICE/BOP-009, Administrative Claims Record System.](#)

[JUSTICE/BOP-10, Access Control Entry/Exit System.2](#)

[JUSTICE/BOP-011, Telephone Activity Record System.](#)

[JUSTICE/BOP-012, Bureau of Prisons, Office of Internal Affairs Investigative Records.](#)

[JUSTICE/BOP-013, Inmate Electronic Message Record System.](#)

[JUSTICE/BOP-014, Employee Assistance Program Record System.](#)

[JUSTICE/BOP-15, Outside Employment Requests Record System.](#)

[JUSTICE/BOP-101, National Institute of Corrections Technical Assistance Resource Project Record System](#)

[JUSTICE/BOP-102, National Institute of Corrections Field Readers List.](#)

[JUSTICE/BOP-103, National Institute of Corrections Academy Record System.](#)

[JUSTICE/BOP-104, National Institute of Corrections Mailing List and Information Center Contacts Record System.](#)

Civil Division

[JUSTICE/CIV-001, Civil Division Case File System.](#)

[JUSTICE/CIV-002, Civil Division Case File System: Customs Litigation.](#)

[JUSTICE/CIV-003, Office of Alien Property File System.](#)

[JUSTICE/CIV-004, Swine Flu Administrative Claim File System.](#)

[JUSTICE/CIV-005, Annuity Broker List System.](#)

[JUSTICE/CIV-006, Consumer Inquiry/Investigatory System.](#)

[JUSYICE/CIV-008, September 11th Victim Compensation Fund of 2001 File System.](#)

Civil Rights Division

[JUSTICE/CRT-001, Central Civil Rights Division Index File and Associated Records Sys](#)

[JUSTICE/CRT-002, Files of Applications for the Position of Attorneys with the Civil Right Division.](#)

[JUSTICE/CRT-003, Civil Rights Case Load Evaluation System-Time Reporting System.](#)

[JUSTICE/CRT-004, Registry of Names of Interested Persons Desiring Notification of Submissions under Section 5 of the Voting Rights Act.](#)

[JUSTICE/CRT-007, Files on Employment Civil Rights Matters Referred by the Equal Employment Opportunity Commission.](#)

[JUSTICE/CRT-009, Civil Rights Division Travel Reports.](#)

Community Relations Service

[JUSTICE/CRS-001, Operational Data Information System.](#)

Criminal Division

[JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records.](#)

[JUSTICE/CRM-002, Criminal Division Witness Security File.](#)

[JUSTICE/CRM-003, File of Names Checked to Determine If Those Individuals Have Been Subject of an Electronic Surveillance.](#)

[JUSTICE/CRM-006, Information File on Individuals and Commercial Entities Known or Suspected of Being Involved in Fraudulent Activities.](#)

[JUSTICE/CRM-008, Name Card File on Department of Justice Personnel Authorized to Access to Classified Files of the Department of Justice.](#)

[JUSTICE/CRM-012, Organized Crime and Racketeering Section, General Index File an](#)

Associated Records.

JUSTICE/CRM-014, Organized Crime and Racketeering Section, Intelligence and Spec Services Unit, Information Request System.

JUSTICE/CRM-018, Registration Files of Individuals Who Have Knowledge of, or Have Received Instruction or Assignment in Espionage, Counterespionage, or Sabotage Serv Tactics of a Foreign Government or of a Foreign Political Party.

JUSTICE/CRM-019, Requests to the Attorney General for Approval of Application to Fe Judges for Electronic Interceptions.

JUSTICE/CRM-021, The Stocks and Bonds Intelligence Control Card File System.

JUSTICE/CRM-022, Witness Immunity Records.

JUSTICE/CRM-025, Tax Disclosure Index File and Associated Records

JUSTICE/CRM-026, Index of Prisoners Transferred Under Prisoner Transfer Treaties.

JUSTICE/CRM-027, Office of Special Investigations (OSI) Displaced Persons Listings.

JUSTICE/CRM-028, Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence and Operations Center System.

Drug Enforcement Administration

JUSTICE/DEA-001, Air Intelligence Program.

JUSTICE/DEA-003, Automated Records and Consolidated Orders System/Diversion An and Detection System (ARCOS/DADS).

JUSTICE/DEA-005, Controlled Substances Act Registration Records (CSA).

JUSTICE/DEA-007, International Intelligence Data Base.

[JUSTICE/DEA-008, Investigative Reporting and Filing System.](#)

[JUSTICE/DEA-009, Medical Records.](#)

[JUSTICE/DEA-010, Planning and Inspection Division Records.](#)

[JUSTICE/DEA-011, Operations Files.](#)

[JUSTICE/DEA-012, Registration Status/Investigation Records.](#)

[JUSTICE/DEA-013, Security Files.](#)

[JUSTICE/DEA-014, System to Retrieve Information from Drug Evidence \(STRIDE/Ballis](#)

[JUSTICE/DEA-015, Training Files.](#)

[JUSTICE/DEA-016, Drug Enforcement Administration Accounting System \(DEAAS II\).](#)

[JUSTICE/DEA-017, Grants of Confidentiality Files \(GCF\).](#)

[JUSTICE/DEA-018, Applicant Investigations \(DAI\).](#)

[JUSTICE/DEA-020, Essential Chemical Reporting System.](#)

[JUSTICE/DEA-021, DEA Aviation Unit Reporting System.](#)

[JUSTICE/DEA-022, EPIC Seizure System \(ESS\).](#)

[JUSTICE/DEA-023, Clerical, Technical and Professional \(CTAP\) Program Files.](#)

[JUSTICE/DEA-027, DEA Employee Profile System \(DEPS\).](#)

[JUSTICE/DEA-028, Regional Automated Intelligence Data System \(RAIDS\).](#)

[JUSTICE/DEA-030, Agent Recruit Assessment Program.](#)

[JUSTICE/DEA-999, DEA Appendix 1—List of Record Location Addresses](#)

Executive Office for Immigration Review

[JUSTICE/EOIR-001, Records and Management Information Systems.](#)

[JUSTICE/EOIR-999, Appendix to Executive Office for Immigration Review System of Re](#)

Federal Bureau of Investigation

[JUSTICE/FBIBRU, Blanket Routine Uses \(BRU\) Applicable to More Than One FBI Private System of Records.](#)

[JUSTICE/FBI-001, National Crime Information Center \(NCIC\).](#)

[JUSTICE/FBI-002, The FBI Central Records System.](#)

[JUSTICE/FBI-003, Bureau Mailing Lists.](#)

[JUSTICE/FBI-006, Electronic Surveillance \(ELSUR\) Indices.](#)

[JUSTICE/FBI-007, FBI Automated Payroll System.](#)

[JUSTICE/FBI-008, Bureau Personnel Management System \(BPMS\).](#)

[JUSTICE/FBI-009, Fingerprint Identification Records System \(FIRS\).](#)

[JUSTICE/FBI-010, Employee Travel Vouchers and Individual Earning Records.](#)

[JUSTICE/FBI-011, Employee Health Records.](#)

[JUSTICE/FBI-012, Time Utilization Record-Keeping \(TURK\) System.](#)

[JUSTICE/FBI-013, Security Access Control System \(SACS\).](#)

[JUSTICE/FBI-014, FBI Alcoholism Program.](#)

[JUSTICE/FBI-015, National Center for the Analysis of Violent Crime \(NCAVC\).](#)

[JUSTICE/FBI-016, FBI Counterdrug Information Indices System \(CIIS\).](#)

[JUSTICE/FBI-017, National DNA Index System \(NDIS\).](#)

[JUSTICE/FBI-018, National Instant Criminal Background Check system \(NICS\).](#)

[JUSTICE/FBI-019, Terrorist Screening Records System.](#)

[JUSTICE/FBI-020, Law Enforcement National Data Exchange \(N-DEx\).](#)

[JUSTICE/FBI-999, Appendix of Field Divisions and Legal Attaches for the Federal Bureau of Investigation Field Divisions.](#)

Foreign Claims Settlement Commission

[JUSTICE/FCSC-1, Indexes of Claimants \(Alphabetical\).](#)

[JUSTICE/FCSC-3, Certifications of Awards.](#)

[JUSTICE/FCSC-4, China, Claims Against.](#)

[JUSTICE/FCSC-5, Civilian Internees \(Vietnam\).](#)

[JUSTICE/FCSC-8, Cuba, Claims Against.](#)

[JUSTICE/FCSC-9, Czechoslovakia, Claims Against.](#)

[JUSTICE/FCSC-10, East Germany, Registration of Claims Against.](#)

[JUSTICE/FCSC-11, Federal Republic of Germany, Questionnaire Inquiries from.](#)

[JUSTICE/FCSC-12, Hungary, Claims Against \(2nd Program\).](#)

[JUSTICE/FCSC–14, Micronesia, Claims Arising in.](#)

[JUSTICE/FCSC–16, Prisoners of War \(Pueblo\).](#)

[JUSTICE/FCSC–17, Prisoners of War \(Vietnam\).](#)

[JUSTICE/FCSC–19, Soviet Union, Claims Against.](#)

[JUSTICE/FCSC–21, German Democratic Republic, Claims Against.](#)

[JUSTICE/FCSC–23, Vietnam, Claims for Losses Against.](#)

[JUSTICE/FCSC–24, Ethiopia, Claims for Losses Against.](#)

[JUSTICE/FCSC–25, Egypt, Claims Against.](#)

[JUSTICE/FCSC–26, Albania, Claims Against.](#)

[JUSTICE/FCSC–27, Germany, Holocaust Survivors' Claims Against.](#)

[JUSTICE/FCSC–28, Iraq, Registration of Potential Claims Against.](#)

[JUSTICE/FCSC–29, Libya, Claims Against.](#)

Foriegn Terrorist Tracking Task Force

[JUSTICE/FTTTF–001, Flight Training Candidates File System.](#)

Immigration and Naturalization Service

[JUSTICE/INS–005, INS Image Storage and Retrieval System \(ISRS\). JUSTICE/INS–007 Orphan Petitioner Index and Files.](#)

[JUSTICE/INS–011, Password Issuance and Control System \(PICS\).](#)

[JUSTICE/INS–015, Port of Entry Office Management Support System \(POMS\).](#)

[JUSTICE/INS-016, Secondary Verification Automated Log \(SVAL\).](#)

[JUSTICE/INS-018, Automated Data Processing Equipment Inventory Management System \(AMIS\).](#)

[JUSTICE/INS-030, Job Swap/Job Exchange System \(JOBX\).](#)

[JUSTICE/INS-999, INS Appendix: List of Principal Offices of Immigration and Naturalization Service.](#)

INTERPOL—United States National Central Bureau

[JUSTICE/Interpol-001, The INTERPOL—United States National Central Bureau \(USNC\) Records System.](#)

Justice Management Division

[JUSTICE/JMD-002, Controlled Substances Act Nonpublic Records.](#)

[JUSTICE/JMD-003, Department of Justice Payroll System.](#)

[JUSTICE/JMD-006, Debt Collection Management System.](#)

[JUSTICE/JMD-007, Accounting System for the Offices, Boards and Divisions and the United States Marshals Service.](#)

[JUSTICE/JMD-009, Debt Collection Offset Payment System.](#)

[JUSTICE/JMD-012, Department of Justice \(DOJ\) Call Detail Records.](#)

[JUSTICE/JMD-014, Security Access Control System \(SACS\).](#)

[JUSTICE/JMD-016, Employee Assistance Program \(EAP\) Counseling and Referral Records.](#)

[JUSTICE/JMD-017, Department of Justice \(DOJ\) Employee Transportation Management System.](#)

[JUSTICE/JMD-021, Department of Justice \(DOJ\) Staffing and Classification System.](#)

[JUSTICE/JMD-022, Department of Justice Consolidated Asset Tracking System \(CATS\)](#)

[JUSTICE/JMD-023, Federal Bureau of Investigation Whistleblower Case Files.](#)

[JUSTICE/JMD-024, Attorney Student Loan Repayment Program Applicant Files.](#)

Environment and Natural Resources Division

[JUSTICE/ENRD-001, Appraisers, Approved Attorneys, Abstractors and Title Companies Database System.](#)

[JUSTICE/ENRD-003, Environment and Natural Resources Division Case and Related F System.](#)

National Drug Intelligence Agency

[JUSTICE/NDIC-001, National Drug Intelligence Center Data Base.](#)

Office of the Attorney General

[JUSTICE/OAG-001, General Files Systems of the Office of the Attorney General.](#)

Office of the Associate Attorney General

[JUSTICE/ASG-001, General Files System of the Office of the Associate Attorney Gener](#)

Office of the Deputy Attorney General

[JUSTICE/DAG-003, Drug Enforcement Task Force Evaluation and Reporting System.](#)

[JUSTICE/DAG-006, Presidential Appointee Candidate Records System.](#)

[JUSTICE/DAG-007, Presidential Appointee Records System.](#)

[JUSTICE/DAG-008, Special Candidates for Presidential Appointments and Noncareer S](#)

[Positions Records System.](#)

[JUSTICE/DAG-009, Summer Intern Program Records System.](#)

[JUSTICE/DAG-010, United States Judge and Department of Justice Presidential Appoi
Records.](#)

[JUSTICE/DAG-011, Miscellaneous Attorney Personnel Records System.](#)

[JUSTICE/DAG-013, General Files System of the Office of the Deputy Attorney General](#)

Office of Community Oriented Policing Services (COPS)

[JUSTICE/COPS-001, Police Corps System.](#)

National Security Division

[JUSTICE/NSD-001, Foreign Intelligence and Counterintelligence Records System.](#)

[JUSTICE/NSD-002, Registration and Informational Material Files Under the Foreign Ag
Registration Act of 1938.](#)

[JUSTICE/NSD-003, Registration Files of Individuals Who Have Knowledge of, or Have
Received Instruction or Assignment in, Espionage, Counterespionage, or Sabotage Ser
Tactics of a Foreign Government or of a Foreign Political Party.](#)

Office of the Inspector General

[JUSTICE/OIG-001, Office of the Inspector General Investigative Records.](#)

[JUSTICE/OIG-004, Office of the Inspector General Employee Training Records.](#)

[JUSTICE/OIG-005, Office of the Inspector General Firearms Qualification System.](#)

Office of Justice Programs

[JUSTICE/OJP-001, Equipment Inventory.](#)

[JUSTICE/OJP-004, Grants Management Information System \(PROFILE\).](#)

[JUSTICE/OJP-005, Financial Management System.](#)

[JUSTICE/OJP-006, Congressional and Public Affairs System.](#)

[JUSTICE/OJP-007, Public Information System.](#)

[JUSTICE/OJP-008, Civil Rights Investigative System.](#)

[JUSTICE/OJP-009, Federal Advisory Committee Membership Files.](#)

[JUSTICE/OJP-010, Technical Assistance Resource Files.](#)

[JUSTICE/OJP-011, Registered Users File-National Criminal Justice Reference Service \(NCJRS\).](#)

[JUSTICE/OJP-012, Public Safety Officers Benefits System.](#)

[JUSTICE/OJP-013, Denial of Federal Benefits Clearinghouse System \(DEBAR\).](#)

[JUSTICE/OJP-14, Victims of International Terrorism Expense Reimbursement Program](#)

Office of Legal Counsel

[JUSTICE/OLC-001, Attorney Assignment Reports.](#)

[JUSTICE/OLC-002, Office of Legal Counsel Central File.](#)

Office of Legal Policy

[JUSTICE/OLP-002, United States Judges Records System.](#)

[JUSTICE/OLP-003, General Files System of the Office of Legal Policy.](#)

Office of Pardon Attorney

[JUSTICE/OPA-001, Executive Clemency Case Files/Executive Clemency Tracking Syst](#)

Office of Professional Responsibility:

[JUSTICE/OPR-001, Office of Professional Responsibility Record Index.](#)

Office of Public Information

[JUSTICE/OPI, News Release, Document and Index System.](#)

U.S. Parole Commission

[JUSTICE/PRC-001, Docket, Scheduling and Control.](#)

[JUSTICE/PRC-003, Inmate and Supervision Files.](#)

[JUSTICE/PRC-004, Labor and Pension Case, Legal File and General Correspondence System.](#)

[JUSTICE/PRC-005, Office Operation and Personnel System.](#)

[JUSTICE/PRC-006, Statistical, Educational and Developmental System.](#)

[JUSTICE/PRC-007, Workload Records, Decision Result, and Annual Report System.](#)

Office of Special Counsel for Immigration-Related Unfair Employment Practices (O

[JUSTICE/OSC 001, Central Index File and Associated Records.](#)

[JUSTICE/OSC-003, Special Counsel for Immigration Related Unfair Employment Practi
Travel Reports.](#)

Office of Special Counsel--Waco

[JUSTICE/OSCW-001, CaseLink Document Database for Office of Special Counsel—W](#)

Tax Division

[JUSTICE/TAX-001, Criminal Tax Case Files, Special Project Files, Docket Cards, and Associated Records.](#)

[JUSTICE/TAX-002, Tax Division Civil Tax Case Files, Docket Cards, and Associated Re](#)

[JUSTICE/TAX-003, Files of Applications for Attorney and Non-Attorney Positions with th](#)
[Division.](#)

United States Attorneys' Office

[JUSTICE/USA-001, Administrative File.](#)

[JUSTICE/USA-002, A. U.S.A. Applicant Files.](#)

[JUSTICE/USA-003, Citizen Complaint Files.](#)

[JUSTICE/USA-005, Civil Case Files.](#)

[JUSTICE/USA-006, Consumer Complaints.](#)

[JUSTICE/USA-007, Criminal Case Files.](#)

[JUSTICE/USA-009, Kline-District of Columbia and Maryland – Stock and Land Fraud](#)
[Interrelationship Filing System.](#)

[JUSTICE/USA-010, Major Crimes Division Investigative Files.](#)

[JUSTICE/USA-011, Prosecutor's Management Information System \(PROMIS\).](#)

[JUSTICE/USA-012, Security Clearance Forms for Grand Jury Reporters.](#)

[JUSTICE/USA-013, U.S. Attorney, District of Columbia Superior Court Operation, Crimi](#)
[Files, including but not limited to the following subsystems: \(a\) Criminal file folder \(USA](#)
[\(b\) Criminal File Folder \(USA-33\), \(c\) Criminal Docket Card \(USA-T7\), and \(d\) Index.](#)

[JUSTICE/USA-014, Pre-Trial Diversion Program Files.](#)

[JUSTICE/USA-015, Debt Collection Enforcement System.](#)

[JUSTICE/USA-016, Assistant United States Attorneys Applicant Records System.](#)

[JUSTICE/USA-017, Appointed Assistant United States Attorneys Personnel System.](#)

[JUSTICE/USA-018, United States Attorney's Office, *Giglio* Information Files.](#)

[JUSTICE/USA-020, Employee Assistance Program \(EAP\) Counseling and Referral Re](#)

[JUSTICE/USA-999, Appendix of United States Attorney Office Locations.](#)

U.S. Marshals Service

[JUSTICE/USM-001, U.S. Marshals Service Badge and Credentials File.](#)

[JUSTICE/USM-002, Internal Affairs System.](#)

[JUSTICE/USM-004, Special Deputation Files.](#)

[JUSTICE/USM-005, U.S. Marshals Service Prisoner Processing and Population Management/Prisoner Tracking System \(PPM/PTS\).](#)

[JUSTICE/USM-006, United States Marshals Service Training Files.](#)

[JUSTICE/USM-007, Warrant Information Network \(WIN\).](#)

[JUSTICE/USM-008, Witness Security Files Information System.](#)

[JUSTICE/USM-009, Inappropriate Communications/Threat Information System.](#)

[JUSTICE/USM-010, Judicial Facility Security Index System.](#)

[JUSTICE/USM-011, Judicial Protection Information System.](#)

[JUSTICE/USM-013, U.S. Marshals Service Administrative Proceedings, Claims and Civil Litigation Files.](#)

[JUSTICE/USM-014, Joint Automated Booking Stations \(JABS\).](#)

[JUSTICE/USM-015, U.S. Marshals Service \(USMS\) Employee Assistance Program \(EAP\) Records.](#)

[JUSTICE/USM-016, U.S. Marshals Service \(USMS\) Key Control Record System.](#)

[JUSTICE/USM-017, Judicial Security Staff Inventory.](#)

[JUSTICE/USM-018, United States Marshals Service Alternative Dispute Resolution \(ADR\) and Database Tracking System.](#)

[JUSTICE/USM-019, Merit Promotion Open Season Records System \(MPOS\).](#)

[JUSTICE/USM-999, Appendix to U.S. Marshals Systems of Records.](#)

U.S. Trustees

[JUSTICE/UST-001, Bankruptcy Case Files and Associated Records.](#)

[JUSTICE/UST-002, Bankruptcy Trustee Oversight Records.](#)

[JUSTICE/UST-003, U.S. Trustee Program Timekeeping Records.](#)

[JUSTICE/UST-004, U.S. Trustee Program Case Referral System.](#)

[JUSTICE/UST-005, Credit Counseling and Debtor Education Files and Associated Records.](#)

[Privacy Act Regulations](#)

[Privacy Act Regulations—Bureau of Prisons](#)

[Privacy Act Regulations—Foreign Claims Settlement Commission](#)

[Federal Acquisition Regulation \(FAR\)](#)

[\[TOP\]](#)

Systems of Records Published Between January 2, 2008 and December 31, 2009

2009

[JUSTICE/DOJ-014, Employee Directory Systems for the Department of Justice: Novem](#)

Criminal Division

2009

[JUSTICE/CRM-028, Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence and Operations Center System: June 3](#)

Environment and Natural Resources Division

2008

[JUSTICE/ENRD-002, Personnel Locator System, Environment and Natural Resources I
July 10](#)

Foreign Claims Settlement Commission

2009

[JUSTICE/FCSC-29, Libya, Claims Against: January 14](#)

[\[TOP\]](#)

Statement of Routine Uses for All Systems of Records

Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses:

Records may be disclosed to appropriate agencies, entities, and persons when

(1) The Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

(2) The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and

(3) The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Administrative Offices

[\[TOP\]](#)

DEPARTMENT OF JUSTICE—001

System Name:

Accounting Systems for the Department of Justice (DOJ).

Security Classification:

The DOJ Accounting Systems may be Sensitive But Unclassified (SBU) or Classified.

System Locations:

Justice Management Division, 950 Pennsylvania Ave., NW., Washington, DC 20530 [Internal Web site: www.usdoj.gov]; Central Offices of the Bureau of Prisons (BOP) at 320 1st St

Washington, DC 20534 and Federal Prison Industries (FPI) at 400 1st St., NW., Washington, DC 20534 [Internet Web site: www.UNICOR.Gov]; and at any BOP/FPI Regional Offices and at any of the BOP/FPI facilities at addresses provided in 28 CFR part 503 [and at the BOP Internet Web site: www.bop.gov]; Headquarters of the Drug Enforcement Administration, Office of Finance, 700 Army Navy Drive, Arlington, VA., 22202; and at DEA field offices as detailed in DEA-999 [and at the DEA Internet Web site: www.dea.gov]; Federal Bureau of Investigation (FBI) Headquarters at 935 Pennsylvania Ave., NW., Washington, DC 20535 and at FBI field offices as detailed in Justice/FBI-999 [and at the FBI Internet Web site: www.fbi.gov]; Office of Justice Programs (OJP), 810 7th Street, NW., Washington, DC 20531 [Internet Web site: www.ojp.gov]; U.S. Marshals Service (USMS), CS-3, 11th Floor, Washington, DC 20530-1000; and at 94 district offices of the USMS [listed at the USMS Internet Web site: www.usms.gov]; Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), 650 Massachusetts Ave., NW., Washington, DC 20226 and at field offices [listed at the ATF Internet Web site: www.atf.gov].

Categories of Individuals Covered by the System:

Individuals/persons (including DOJ employees; and including current and former inmates under the custody of the Attorney General) who are in a relationship, or who seek a relationship, with the DOJ or a component thereof—a relationship that may give rise to accounts receivable, an accounts payable, or to similar accounts such as those resulting from a grantee/grantor relationship; and federal debtors, including those who have received overpayments through direct financial assistance, those who owe debts of restitution based on civil or criminal judgments entered by federal courts, and those who have obtained insured loans from federal agencies, and whose delinquent debts have been sent to federal agencies to the DOJ for enforced collection through litigation. Included may be:

(a) Those for whom vouchers (except payroll vouchers for DOJ employees) are submitted to the DOJ requesting payment for goods or services rendered including vendors, contractors, experts, witnesses, court reporters, travelers, and employees;

(b) Those to whom the DOJ is indebted or who may have a claim against the DOJ, including those named in (a) above;

(c) Those who are indebted to DOJ, e.g., those receiving goods, services, or benefits from the DOJ; those who are liable for damage to Government property; those indebted for travel/transfer advances and overpayments; and those owing administrative fees and/or

assessments; and

(d) Those who apply for DOJ benefits, funds, and grants.

(e) Those who have made partial or full payments to be applied to their federal debt.

Categories of Records in the System:

(1) All documents used to reserve, obligate, process, and effect collection or payment of e.g., vouchers (excluding payroll vouchers), invoices, purchase orders, travel advances, travel/transfer vouchers and other such documentation reflecting information about: (a) Payments due or made to, (b) claims made or debts owed by the individuals covered by system, including fees, fines, penalties, overpayments, and/or other assessments; all documents used to comply with reporting regulations of the Internal Revenue Service or Department of Treasury; and (3) all documentation and information pertaining to the repayments made by or on the behalf of federal debtors against their debts and the disbursement or transfer of those payments by DOJ to the appropriate recipients.

Authority for Maintenance of the System:

31 U.S.C. 3512; 44 U.S.C. 3101.

Purpose of the System:

This system of records is used by DOJ officials to maintain information adequate to ensure financial accountability of the individuals covered by this system; provide an accounting reporting of DOJ financial activities; meet both internal and external audit and reporting requirements; maintain an accounts receivable and accounts payable; and otherwise administer these and any other related financial and accounting responsibilities.

Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses:

DOJ may disclose relevant information as follows:

(1) To the Secretary of the Treasury to effect disbursement of authorized payments.

(2) To any Federal agency or to any individual or organization for the purpose of performing audit or oversight operations of the DOJ and to meet related reporting requirements.

(3) To appropriate officials and employees of a Federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit.

(4) To Federal, State, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

(5) Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, foreign, or tribal, law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.

(6) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

(7) In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator holds the records to be relevant to the proceeding.

(8) To the news media and the public pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(9) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record.

(10) To the National Archives and Records Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(11) To any Federal, State, or local agency, or tribal authority, which has a financial or legitimate need for the information to perform official duties; or, similarly, to obtain information which would enable the Department to perform its official duties. Examples include: to permit such agency to perform accounting functions or to report to the Department of the Treasury regarding the status of a Federal employee/contractor debt owed to such Federal, State, or local agency; to report on the status of Department efforts to collect such debt; to obtain information necessary to identify a Federal employee/contractor indebted to such agency; to provide information regarding the location of such debtor; or to obtain information which would permit the Department to confirm a debt and/or offset a payment otherwise due a Federal employee/contractor after any appropriate due process steps have been taken.

(12) To any Federal, State, local, or foreign agency, or tribal authority, or to any individual or organization, if there is reason to believe that such agency, authority, individual, or organization possesses information relating to a debt, the identity or location of the debtor, the debtor's ability to pay; or relating to any other matter which is relevant and necessary to the settlement, effective litigation and enforced collection of a debt; or relating to the civil action, trial or proceeding concerning the collection of such debt; and if the disclosure is reasonably necessary to obtain such information and/or obtain cooperation of a witness or agency;

(13) To the U.S. Department of the Treasury, the U.S. Department of Defense, the U.S. Postal Service, or other disbursing agencies, in order to effect administrative, salary, or tax refund offset against Federal payments to collect a delinquent claim or debt owed the United States or a State; to satisfy a delinquent child support debt; or to effect other actions required or permitted by law to collect such debt.

(14) To the U.S. Department of the Treasury any information regarding adjustments to delinquent debts, such as voluntary payments which decrease the debt, changes in the status resulting from bankruptcy, any increase in the debt, or any decrease in the debt resulting from changes in agency statutory requirements.

(15) To employers to effect salary or administrative offset to satisfy a debt owed the United States by the debtor or, when other collection efforts have failed, to the Internal Revenue

Service (IRS) to effect an offset against Federal income tax refund due.

(16) To employers to institute administrative wage garnishments to recover debts owed United States.

(17) To debt collection centers designated by the U.S. Department of the Treasury (or to person with whom the DOJ has entered into a contract) to locate or recover assets of the debtor or for sale of a debt; or to otherwise recover indebtedness owed.

(18) In accordance with regulations issued by the Secretary of the Treasury to implement the Debt Collection Improvement Act of 1996, to publish or otherwise publicly disseminate information regarding the identity of the person and the existence of a non-tax debt in order to take direct actions under the law toward delinquent debtors that have assets or income sufficient to pay their delinquent non-tax debts, but only upon taking reasonable steps to ensure the accuracy of the identity of a debtor; upon ensuring that such debtor has had an opportunity to verify, contest, and compromise a non-tax debt; and with the review of the Secretary of the Treasury.

(19) To the IRS for reporting a discharged debt as potential taxable income.

(20) To the IRS to obtain taxpayer mailing addresses for debt collection use. These taxpayer mailing addresses may be disclosed

(a) To private collection contractors to locate a taxpayer and to collect or compromise a debt against, or debt of, the taxpayer, and

(b) To consumer or commercial reporting agencies to obtain a credit report.

(21) To the Department of Health and Human Services, and the Department of Labor, for computer matching in order to obtain names (including names of employees), name changes, names of employers, Taxpayer Identification Numbers, addresses (including addresses of employers) and dates of birth for the purpose of verifying identities in order to pursue the collection of debts.

(22) To other Federal or State agencies as required by law.

(23) To a consumer or commercial reporting agency in accordance with the Debt Collec

Improvement Act of 1996.

(24) To contractors, grantees, experts, consultants, students, and others performing or on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or records.

(25) To a person or to an entity (e.g., the U. S. Department of the Treasury and/or a corporate or commercial reporting agency), Taxpayer Identification Numbers (TIN's), to report on delinquent debt and/or to pursue the collection of debt, or where otherwise necessary or required, e.g., U. S. Department of the Treasury for disbursement of payments authorized—provided such disclosure is not otherwise prohibited by Section 6103 of the Internal Revenue Code, or other law.

(26) The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee, if necessary, may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Disclosure to Consumer Reporting Agencies:

Only as noted in Routine Use 20(b) and Routine Use 23 in the *Federal Register* notice of 3, 2004 (69 FR 31406).

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing Records in the System:

Storage:

Magnetic disks, magnetic tapes, microfiche, microfilm, file folders, and digitized images, other media.

Retrievability:

Document number, name, taxpayer identification number, digital identifiers, batch, or other identifiers.

Safeguards:

All data will be protected in accordance with applicable DOJ and federal guidance, policies, and directives based on the security classification of the information/system. Access is limited to DOJ personnel with a need to know. Access to computerized information is controlled by passwords, or similar safeguards, which are issued only to authorized personnel. Records are retained in the form of digitized images on a server to which limited workstations have access. Passwords control access to the server from these workstations. Paper records, and some computerized media, are kept in locked files of locked offices during off duty hours. In addition, servers, workstations, and offices are located in controlled-access buildings.

Retention and Disposal:

Records are retained and disposed of in accordance with General Records Schedules 6 and 7.

System Manager(s) and Addresses:

DAAG/Controller, Finance Staff, Justice Management Division (JMD), U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530.

Director, Federal Bureau of Prisons (BOP), 320 First St., NW., Washington, DC 20534.
Director, BOP, is also system manager for Federal Prison Industries (FPI).]

Chief Financial Officer, Financial Management Division, Drug Enforcement Administration (DEA), 700 Army Navy Drive, Arlington, VA 22202.

Director, Federal Bureau of Investigation (FBI), 935 Pennsylvania Ave., NW., Washington, DC 20535.

Director, Accounting Division, Office of Justice Programs (OJP), 810 7th Street, NW., Washington, DC 20531.

Chief, Finance Staff, Management and Budget Division, U.S. Marshals Service, CS-3, 1

Floor, Washington, DC 20530–1000.

Office of Management/Chief Financial Officer, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Ave., NW., Washington, DC 20226.

Notification Procedures:

Same as record access procedures.

Record Access Procedures:

Request for access to records in this system must be in writing and should be addressed as follows:

JMD: For records of the Offices, Boards and Divisions, address requests to the system manager named above for JMD.

OJP: Address request to the system manager named above.

BOP: Address requests to the Assistant Director, Administration Division, 320 First Street, NE, Washington, DC 20534.

FPI: Address requests to Assistant Director, Federal Prison Industries, 400 First Street, NE, Washington, DC 20534.

USMS: Address requests to the system manager named above, attention: FOI/PA Office.

DEA: Address requests to the system manager named above.

FBI: Address requests to the system manager named above.

ATF: Address request to Disclosure Division, Privacy Act Request, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW., Washington, DC 20226.

The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's name and address.

full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury. If known, the requester should identify the date or year in which a debt was incurred, e.g., date of invoice or purchase

Contesting Record Procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Record Access Procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment, such as tax return information. A determination whether a record may be amended will be made at the time a request is received.

Record Source Categories:

Operating personnel, individuals covered by the system, and Federal agencies.

Exemptions Claimed for the System:

None.

[\[TOP\]](#)

JUSTICE-002

System name:

Department of Justice (DOJ) Computer Systems Activity and Access Records, DOJ-002

System location:

Department of Justice offices (and other sites utilized by the Department of Justice) throughout the world.

Categories of individuals covered by the system:

Individuals who access DOJ network computers or mainframe/enterprise servers, including

individuals who send and receive electronic communications, access Internet sites, or a system databases, files, or applications from DOJ computers or sending electronic communications to DOJ computers; and individuals attempting to access DOJ computer systems without authorization.

Categories of records in the system:

Records in this system of records may include: Records on the use of the interoffice and Internet e-mail systems, including the e-mail address of the sender and receiver of the e-mail message, subject, date, and time; records on user access to DOJ's office automation network including user ID, date and time of log on and log off, and denials of access to unauthorized files or directories; records of Internet access from a DOJ computer, such as the Internet Protocol (IP) address of the computer being used to initiate the Internet connection, the files accessed, date, and time; records relating to mainframe/enterprise server access, such as user ID of the individual accessing the mainframe, date and time, and the process being run on the mainframe; records relating to verification or authorization of an individual's access to system files, or applications, such as user IDs, passwords, user names, title, and agency.

Logs of Internet access from a DOJ computer do not contain names or similar personal identifiers. However, for official government business purposes, a name may be associated with an IP address.

Authority for maintenance of the system:

The Computer Security Act of 1987, 40 U.S.C. 1441 note, requires Federal Agencies to protect the security and privacy of their computer systems.

Purpose(s):

The underlying raw data in this system of records is used by DOJ systems and security personnel, or persons authorized to assist these personnel, to plan and manage system services and to otherwise perform their official duties. Authorized DOJ managers may use records in this system to investigate improper access or other improper activity related to computer system access; to initiate disciplinary or other such action; and/or where the record(s) may appear to indicate a violation or potential violation of the law, to refer such record(s) to the appropriate investigative arm of DOJ, or other law enforcement agency for investigation.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information may be made available in accordance with the disclosure provisions cited below.

1. To members of Congress or staff to respond to inquiries made on behalf of individual constituents who are record subjects.
2. To representatives of the General Services Administration and/or the National Archives Records Administration who are conducting records management inspections under the authority of 44 U.S.C. 2904 and 2906.
3. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.
4. To a Federal, state, local, tribal or foreign agency, or a private contractor, in connection with the hiring or retention of any employee; the issuance of a security clearance; the conduct of a security or suitability investigation or pursuit of other appropriate personnel matter; the reporting of an investigation on an employee; the letting of a contract; or the issuance of a grant, license, or other benefit to an employee by the agency, but only to the extent that the information disclosed is relevant and necessary to the agency's decision on the matter.
5. To provide information to any person(s) authorized to assist in an approved investigation of the improper usage of DOJ computer systems.
6. To an actual or potential party or his or her authorized representative for the purpose of negotiation or discussion on such matters as settlement of the case or matter, or information discovery proceedings.
7. In the event that material in this system of records appears to indicate, either on its face or in conjunction with other information, a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute, or by regulation or order issued pursuant thereto, to a Federal, State, local, tribal, or foreign unit of government charged with the responsibility therefor.

8. In a proceeding before a court or adjudicative body, when any of the following is a party to the litigation or has an interest in litigation and such records are determined by the DOJ to be arguably relevant to the litigation: The DOJ; any employee of the DOJ in his or her official capacity; or any employee of the DOJ in his or her individual capacity where the DOJ has agreed to represent or has authorized private attorneys to represent the employees; or, United States, where the DOJ determines that the litigation is likely to affect it or any of its subdivisions.

9. To contractors, grantees, experts, consultants, detailees, and other non-DOJ employees performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system of records.

10. To other government agencies where required by law.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records are stored in electronic and/or paper form.

Retrievability:

Records may be retrieved by user name, user ID, e-mail address, or other identifying information term employed, depending on the record category. The Department does not usually connect IP addresses with a person. However, in some instances, for official government business purposes, the Department may connect the IP address with an individual, and records may

retrieved by IP address.

Safeguards:

Access is limited to those who have an official need to know. Specifically, only systems security personnel or persons authorized to assist these personnel have access to auto records and magnetic storage media. These records are kept in a locked room with controlled entry. The use of password protection identification features and other automated data processing system protection methods also restrict access. All records are located in buildings with restricted access.

Retention and disposal:

Records of verification, authorization, computer system access, and other activities generated by the system shall be retained no longer than one year, unless required for management review, then destroyed/deleted. (Records retention schedule pending approval by the Attorney General of the United States.)

System manager(s) and address: :

Deputy Assistant Attorney General, Information Resources Management, Justice Management Division, Department of Justice, Washington, DC 20530.

Notification procedure:

To determine whether the system may contain records relating to you, write to the System Manager identified above.

Record access procedures:

Same as "Notification Procedure" above. Provide name, assigned computer location, and description of information being sought, including the time frame during which the records may have been generated. Provide verification of identity as instructed in 28 CFR 16.41(c).

Contesting record procedures:

See "Notification Procedure" and "Record Access Procedure" above. Identify the information

being contested, the reason for contesting it, and the correction requested. In general, this information is computer-generated and is not subject to contest.

Record source categories:

Most records are generated internally, i.e., computer activity logs; individuals covered by the system; and management officials.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE-003

System name:

Correspondence Management Systems (CMS) for the Department of Justice.

System location:

U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530, and all Department of Justice offices throughout the country.

Categories of individuals covered by the system:

Individuals originating, receiving, or named in correspondence (including attachments) to or from the Department or whose correspondence is referred to the Department, or person communicating electronically or by telephone with the Department regarding official business of the Department, including Members of Congress, other government officials, individuals and their representatives; individuals originating, receiving, or named in internal memoranda (including attachments) within the Department, including DOJ employees, contractors, and individuals relating to investigators, policy decisions, or administrative matters of significance to the Department of Justice; in some instances, Department of Justice personnel assigned to handle such correspondence and other matters.

Categories of records in the system:

Correspondence identification (e.g., correspondence's name, address, title, organization control number, date of correspondence, date received, subject); status of response with Department; may include original correspondence, Department's response, office or staff member assigned to handle the matter, referral letters, name and identification of person referring the correspondence, copies of any enclosures, and related materials. Some internal memoranda, e-mail correspondence, and logs/notes of official telephone calls to/by Department staff are also tracked. Records may include case files, litigation materials, and other goods on a given subject or individual. This material varies according to the wide scope of the responsibilities of the Department of Justice. Correspondence identification tracking information, as well as some substantive information on these matters is maintained in an automated database in electronic format and/or paper files. This system does not cover systems of records covered by separately-noticed systems.

Authority for maintenance of the system:

5 U.S.C. 301 and 44 U.S.C. 3101.

Purpose(s):

The System controls and tracks correspondence received or originated by the Department referred to the Department, and action taken by the Department in response to correspondence received, as well as some internal memoranda, action items, e-mail correspondence, and logs/notes of official telephone calls. It also serves as a reference for inquiries and response thereto.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Pursuant to subsection (b)(3) of the Privacy Act, information may be disclosed from this system as follows:

A. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

- B. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of an individual who is the subject of the record
- C. To the General Services Administration and National Archives and Records Administration for records management inspections conducted under the authority of 44 U.S.C. 2904 and
- D. Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, to any civil or criminal law enforcement authority or appropriate agency, whether federal, state, local, foreign, or tribal, charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing a statute, rule, regulation, or order.
- E. In an appropriate proceeding before a court, grand jury, or administrative or regulatory body when records are determined by DOJ to be arguably relevant to the proceeding.
- F. To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.
- G. To a federal agency or entity that requires information relevant to a decision concerning hiring, appointment, or retention of an employee, the issuance of a security clearance, the conduct of a security or suitability investigation, or pursuit of other appropriate personnel matter.
- H. To a federal, state, local, or tribal agency or entity that requires information relevant to a decision concerning the lettering of a letter or permit, the issuance of a grant or benefit; or other need for the information in performance of official duties.
- I. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system's records.
- J. To a former employee of the Department for purposes of: responding to an official inquiry from a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee.

that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding matter within that person's former area of responsibility.

K. To the White House (the President, Vice President, their staffs, and other entities of the Executive Office of the President (EOP)) for Executive Branch coordination of activities that relate to or have an effect upon the carrying out of the constitutional, statutory, or other or ceremonial duties of the President.

L. To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are stored in electronic form and on paper.

Retrievability:

Information can be retrieved by correspondence control number; name of individual; subject matter of topic; or in some cases, by other identifying search term employed.

Safeguards:

Information in these systems is safeguarded in accordance with applicable rules and policies, including the Department's automated systems security and access policies. Tax return information is safeguarded in accordance with 26 U.S.C. 6103. Classified information is appropriately stored in safes and in accordance with other applicable requirements. Information records and technical equipment are maintained in buildings with restricted access. The required use of password protection identification features and other system protection methods also restrict access. Access is limited to those who have an official need for access to perform their official duties.

Retention and disposal:

Records are retained and disposed of in accordance with individual component guidelines approved by the National Archives and Records Administration (SF 115s), and/or pursuant to General Records Schedule 14, or 23, item 8.

System manager(s) and address:

Deputy Assistant Attorney General, Human Resources/Administration, Justice Management Division, 950 Pennsylvania Ave., NW., Washington, DC 20530.

Notification procedure:

Address inquiries to System Manager named above.

Record access procedures:

Requests for access must be in writing and should be addressed to the System Manager named above. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury. Some information may be exempt from access provisions as described in the section entitled "Systems Exempt from Certain Provisions of the Act." An individual who is the subject of a record in the system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment, such as tax return information. Some information may be exempt from contesting record procedures as described in the section entitled "Systems Exempted from Certain Provisions of the Act." An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

Record source categories:

Sources of information contained in these systems include individuals, state, local, tribal and foreign government agencies as appropriate, the executive and legislative branches of the Federal Government, the Judiciary, and interested third parties. The source of the information on the control records contained in these systems is derived from incoming and outgoing correspondence and internal memoranda.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d)(1), (2), (3), (4), (5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (k). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b) and (e) and have been published in the *Federal Register*. These exemptions apply only to the extent that information in a record pertaining to a particular individual is classified to protect national security, or relates to official investigations and law enforcement matters. A determination as to exemption shall be made at the time a request for access or amendment is received.

[\[TOP\]](#)

JUSTICE-004

System name:

Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Request and Administrative Appeals for the Department of Justice.

System location:

United States Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001, and other Department of Justice offices throughout the country.

Categories of individuals covered by the system:

The system encompasses all individuals who submit Freedom of Information Act (FOIA) requests, Privacy Act, and Mandatory Declassification Review Requests and administrative appeals.

Department of Justice; individuals whose requests and/or records have been referred to Department of Justice by other agencies; and in some instances includes attorneys representing individuals submitting such requests and appeals, individuals who are the subjects of such requests and appeals, and/or the Department of Justice personnel assigned to handle such requests and appeals.

Categories of records in the system:

The system consists of records created or compiled in response to FOIA, Privacy Act, and Mandatory Declassification Review requests and administrative appeals and includes: The original requests and administrative appeals; responses to such requests and administrative appeals; all related memoranda, correspondence, notes, and other related or supporting documentation; and, in some instances, copies of requested records and records under administrative appeal.

Authority for maintenance of the system:

The system was established and is maintained pursuant to 5 U.S.C. 301 and 44 U.S.C. to implement the provisions of 5 U.S.C. 552 and 5 U.S.C. 552a, and the applicable executive order(s) governing classified national security information.

Purpose(s):

This system is maintained for the purpose of processing access requests and administrative appeals under the FOIA, access and amendment requests and administrative appeals under the Privacy Act, and requests and administrative appeals for mandatory declassification under the applicable executive order(s) governing classified national security information; the purpose of participating in litigation regarding agency action on such requests and appeals; and for the purpose of assisting the Department of Justice in carrying out any responsibilities under the FOIA, the Privacy Act, and applicable executive orders.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information may be disclosed from this system as follows:

A. To a federal, state, local, or foreign agency or entity for the purpose of consulting with

agency or entity to enable the Department of Justice to make a determination as to the propriety of access to or correction of information, or for the purpose of verifying the identity of an individual or the accuracy of information submitted by an individual who has requested access to or amendment of information.

B. To a federal agency or entity that furnished the record or information for the purpose of permitting that agency or entity to make a decision as to access to or correction of the record or information, or to a federal agency or entity for purposes of providing guidance or advice regarding the handling of particular requests.

C. To a submitter or subject of a record or information in order to obtain assistance to the Department in making a determination as to access or amendment.

D. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system's records.

E. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

F. In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, or tribal law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.

G. To officials and employees of a federal agency or entity which requires information related to a decision concerning the hiring, appointment, or retention of an employee; the issuance of a security clearance; the execution of a security or suitability investigation; the classification of a job; or the issuance of a grant or benefit.

H. To federal, state, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

I. In a proceeding before a court or adjudicative body before which the Department of Justice

authorized to appear when (a) the Department of Justice, or any subdivision thereof, or employee of the Department of Justice in his or her official capacity, or (c) any employee of the Department of Justice in his or her individual capacity where the Department of Justice agreed to represent the employee, or (d) the United States, where the Department of Justice determines that the litigation is likely to affect it or any of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the Department of Justice to be arguably relevant to the litigation.

J. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

K. To the General Services Administration and National Archives and Records Administration records management inspections conducted under the authority of 44 U.S.C. 2904 and

L. To a former employee of the Department of Justice for purposes of: Responding to an inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

M. To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records in this system are stored on paper and/or in electronic form. Records that contain national security information and are classified are stored in accordance with applicable executive orders, statutes, and agency implementing regulations.

Retrievability:

Records are retrieved by the name of the requester or appellant; the number assigned to

request or appeal; and in some instances may be retrieved by the name of the attorney representing the requester or appellant, the name of an individual who is the subject of request or appeal, and/or the name or other identifier of Department of Justice personnel assigned to handle such requests or appeals. Immigration and Naturalization Service records are also retrieved by alien number and social security number.

Safeguards:

Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including the Department's automated systems security and access policies. Classified information is appropriately stored in safes and in accordance with other applicable requirements. In general, records and technical equipment are maintained in buildings with restricted access. The required use of password protection identification features and other system protection methods also restrict access. Access is limited to those officers and employees of the agency who have an official need for access in order to perform their duties.

Retention and disposal:

Records are retained and disposed of in accordance with the National Archives and Records Administration's General Records Schedule 14.

System manager(s) and address:

Associate Director, Office of Information and Privacy, United States Department of Justice
Pennsylvania Avenue, NW., Washington, DC 20530-0001.

Notification procedure:

Records concerning initial requests under the FOIA, the Privacy Act, and the applicable executive order(s) governing classified national security information are maintained by the individual Department of Justice component to which the initial request was addressed or directed. Inquiries regarding these records should be addressed to the particular Department of Justice component maintaining the records, United States Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001.

Records concerning administrative appeals under the FOIA, the Privacy Act, and the applicable executive order(s) governing classified national security information, with the exception of

made to the United States Parole Commission, are maintained by the Office of Information Privacy. Inquiries regarding these records should be addressed to the Office of Information Privacy, United States Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001. Inquiries regarding administrative appeals made to the United States Parole Commission should be addressed to the United States Parole Commission, United States Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001.

Record access procedures:

Requests for access may be made by appearing in person or by writing to the appropriate office indicated in the "Notification Procedures" section, above. The envelope and letter must be clearly marked "Privacy Act Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date of birth. The request must be signed and either notarized or submitted under penalty of perjury. Some information may be exempt from access as described in the section entitled "Systems Exempted from Certain Provisions of the Act." An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination of whether a record may be accessed will be made after a request is received.

Although no specific form is required, you may obtain forms for this purpose from the Federal Mail Referral Unit, Justice Management Division, United States Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001, or on the Department of Justice Web site at www.usdoj.gov/04foia/att_d.htm.

Contesting record procedures:

Individuals seeking to contest or amend information maintained in the system should direct their requests to the appropriate office indicated in the "Notification Procedures" section, stating clearly and concisely what information is being contested, the reasons for contesting, and the proposed amendment to the information sought. Some information may be exempt from contesting record procedures as described in the section entitled "Systems Exempted from Certain Provisions of the Act." An individual who is the subject of a record in this system may seek amendment of those records that are not exempt. A determination of whether a record is exempt from amendment will be made after a request is received.

Record source categories:

Those individuals who submit initial requests and administrative appeals pursuant to the Privacy Act, or the applicable executive order(s) governing classified national security information; the agency records searched in the process of responding to such requests; appeals; Department of Justice personnel assigned to handle such requests and appeals; other agencies or entities that have referred to the Department of Justice requests concerning Department of Justice records, or that have consulted with the Department of Justice regarding the handling of particular requests; and submitters or subjects of records or information have provided assistance to the Department of Justice in making access or amendment determinations.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d)(1), and (4); (e)(1), (2), (3), (5), and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(k). These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k).

Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (e), and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DOJ-005

System Name:

Nationwide Joint Automated Booking System (JABS).

Security Classification:

Sensitive but Unclassified.

System Location:

JABS Program Management Office, Department of Justice, Washington, DC 20530 with collection sites in multiple federal locations.

Categories of Individuals Covered by the System:

Alleged criminal offenders who have been detained, arrested, booked, or incarcerated. The remainder of this notice will refer to all persons covered by the System as "alleged criminal offender" or "arrestee" .

Categories of Records in the System:

Records may include certain generic or "common" data elements which have been collected by an arresting federal agency at its automated booking station (ABS). An agency may book an alleged criminal offender on behalf of another agency which performed the arrest. Such common data (certain data elements) have been identified by law enforcement as those and biographical data routinely collected by the law enforcement community during the booking process, e.g., name, date and place of birth, citizenship, hair and eye color, height and weight, occupation, social security number, place, date and time of arrest and jail location, charge, disposition, any other pertinent information related to known activities relevant to the subject, and any unique to the subject. Finally, such data may include electronic fingerprints, mugshots, pictures of applicable scars, marks, and tattoos.

Authority for Maintenance of the System:

8 U.S.C. 1324 and 1357(f) and (g); 28 U.S.C. 534, 564, 566; 5 U.S.C. 301 and 44 U.S.C. 3601, 3602, 3605, 3606, 3607, 3609, 3610, 3611, 3612, 3613, 3614, 3615, 3616, 3617, 3618, 3619, 3620, 3621, 4003, 4042, 4082, 4086; 26 U.S.C. 7608; and Comprehensive Drug Abuse Prevention and Control Act of 1970 (Pub. L. 91-513), 21 U.S.C. 801 *et seq.* and Reorganizational Plan No. 2 of 1973.

Purpose:

Nationwide JABS enables the conduct of automated booking procedures by participating law enforcement organizations and provides an automated capability to transmit fingerprint image data to the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS), Justice/FBI-009 Fingerprint Identification Records System (FIRS). JABS maintains a repository of common offender data elements for identification of arrestees by participating federal law enforcement organizations. JABS eliminates repetitive booking of offenders for a single arrest and booking, and thereby eliminates the need for duplicate bookings, i.e., the collection of much the same data by multiple agencies in processing activities involving such agencies from arrest through incarceration. In addition,

JABS standardized booking data elements, enabling cross-agency sharing of booking information, enhancing cooperation among law enforcement agencies, and reducing the burden on law enforcement officials and the public by facilitating the rapid and positive identification of offenders.

Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses:

Where necessary and/or appropriate, the DOJ may disclose relevant information from the JABS repository and may allow electronic access as follows:

- a. To authorized federal law enforcement agencies to input and retrieve booking and arrest data on criminal offenders. In addition, the JABS repository may be electronically accessed by these agencies for other law enforcement purposes such as to learn about the arrest of a fugitive wanted in several jurisdictions, to verify the identity of an arrestee, or to assist in criminal investigation activities.
- b. To other judicial/law enforcement agencies, *i.e.*, courts, probation, and parole agencies, to provide direct electronic access to JABS to obtain applicable data which will assist them in performing their official duties.
- c. To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.
- d. In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
- e. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.
- f. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system.

records.

g. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

h. To the news media and the public, pursuant to 28 CFR 50.2, unless it is determined release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

i. To the National Archives and Records Administration (NARA) for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

j. The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee, if necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Disclosure to Consumer Reporting Agencies:

Not Applicable.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing Records in the System:

Storage:

Records are stored in computerized media and printed copies. Any paper records kept by individuals will be appropriately secured.

Retrievability:

Data may be retrieved by name, identifying number, or other data elements.

Safeguards:

Nationwide JABS has a combination of technical elements that, together, integrate into security infrastructure to ensure access is limited to only pre-authorized users. The key technical design elements of this architecture include: Encrypted user authentication, redundant firewalls, virtual private networks, nonrepudiation, data encryption, anti-virus inspection, and intrusion detection capabilities. Access to the systems equipment is limited to pre-authorized personnel through physical access safeguards that are enforced 24 hours a day, seven (7) days a week. Facilities and offices which house computer systems are protected at all times by appropriate locks, security guards, and/or alarm systems.

Retention and Disposal:

- a. Temporary. Delete from the JABS data base 99 years after the date of the first entry.
- b. Fingerprints submitted by law enforcement agencies are removed from the system and destroyed upon the request of the submitting agencies. The destruction of fingerprints under this procedure results in the deletion from the system of all arrest information related to fingerprints.
- c. Fingerprints and related arrest data are removed from the JABS upon receipt of court order for expunction when accompanied by necessary identifying information.

System Manager(s) and Address(es):

JABS Program Management Office, U.S. Department of Justice, Washington, DC 20530

Notification Procedure:

Same as "Record Access Procedure."

Record Access Procedure:

Inquiries must be addressed in writing and should be sent to the JABS Program Management Office, at above address. Provide name, assigned computer location, and a description of the information being sought, including the time frame during which the record(s) may have

generated. Provide verification of identity as instructed in 28 CFR 16.41(d).

Contesting Records Procedure:

Same as above.

Records Source Categories:

The record subject; federal law enforcement personnel; the courts; and medical person

Exemptions Claimed for the System:

Pursuant to 5 U.S.C. 552a(j)(2) and (k)(2), the Attorney General has exempted records system from subsections (c)(3) and (4), (d), (e)(1), (2) and (3), (4)(G) and (H), (e)(5), (e) and (g) of the Privacy Act. Rules were promulgated in accordance with the requirement: U.S.C. 553(b), (c), and (e) and are codified at 28 CFR 16.131.

[\[TOP\]](#)

JUSTICE—006

System name:

Personnel Investigation and Security Clearance Records for the Department of Justice, DOJ-006.

System classification:

Not classified.

System location:

U.S. Department of Justice, 950 Pennsylvania Avenue, NW, Washington, DC 20530, otl Department of Justice Component locations (see system manager listings). Working co records may reside temporarily at locations operated by contractors authorized to provic computer services and other agency functions related to this system of records.

Categories of individuals covered by the system:

Current and former employees of the Department, including but not limited to full and part-time employees, interns, detailees, volunteers, and task force personnel;

Current and former contractor employees and prospective contractor employees, for whom an investigation is initiated and/or conducted; Current and former Congressional staff personnel, Executive Office of National Security personnel, Office of Independent Counsel personnel, Special Counsel personnel, Foreign Intelligence Surveillance Act judges and staff, Presidential Transition personnel, and other individuals employed by or performing services for the Federal Government who require background investigations;

Any or all persons associated with and/or acting for the defense or for the courts in a criminal proceeding involving classified information and any Department component;

Applicants for paid or unpaid employment with the Department for whom an investigation is initiated and/or conducted; and

Individuals who have been investigated for purposes of determining eligibility for access to sensitive or national security information.

Categories of records in the system:

Identifying information regarding the individuals in the Categories of Individuals above, including one or more of the following: (1) Standard Form 86 "Questionnaire for National Security Positions," Standard Form 85P "Questionnaire for Public Trust Positions," Standard Form 85P-S "Supplemental Questionnaire for Selected Positions," and/or Standard Form 85 "Questionnaire for Non-Sensitive Positions" and predecessor and successor forms of this type; (2) Copies of investigative reports from the Office of Personnel Management (OPM), Federal Bureau of Investigation (FBI), and/or other Federal investigative agencies; (3) Correspondence, information, and other supporting documentation related to the investigation and adjudication for public trust and national security information positions (references to classified and national security information include Sensitive Compartmented Information); (4) Form DOJ-555 "Disclosure and Authorization Pertaining to Consumer Credit Pursuant to the Fair Credit Reporting Act" and other consent or waiver forms, and the results of credit checks; (5) Waivers of the pre-employment background investigation requirement; (6) Records of security clearance certifications; (7) Other information relating to the loyalty and trustworthiness of the individual, or relevant to the individual's eligibility for access to national security information.

security information; and (8) Records reviewed by the Access Review Committee (ARC) generated in connection with the ARC appeals procedure (Executive Order 12968, Sect 5.2.(a)(7)).

Authority for maintenance of the system:

Presidential Executive Orders 10450, "Security Requirements for Government Employment" and 12968, "Access to Classified Information," and the Classified Information Procedure Act of 1980.

Purpose(s):

Records in this system are used to determine the loyalty, trustworthiness, suitability, eligibility and/or qualifications of employees for initial or continued employment in the Department of Justice, and for employment in sensitive positions involving eligibility and continued eligibility for access to classified information. The records are also used to make similar suitability and security determinations regarding the employment of contractors to perform a service for the Department and to establish the trustworthiness for access to classified information of persons associated with and/or acting for the court or the defense during criminal proceedings, and in other specified cases where individuals employed by or performing services for the Federal Government require background investigations, including during Presidential transitions. Records in this system are also used by the Access Review Committee when an appeal is made to the ARC to review a security clearance denial or revocation pursuant to E.O. 12968. Records in this system are also used to track the status and types of investigations, the results of clearances and level of clearances.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Disclosure determinations regarding any investigative records from an OPM or FBI investigation will be made only in accordance with the investigating agency's disclosure policies.

Records or information in this system of records may be disclosed to the following parties if it has been determined by the Department of Justice that such a need exists:

(a) Designated officers and employees of agencies, offices, and other establishments in the executive, legislative, and judicial branches of the Federal Government, in connection with

hiring or continued employment of an employee or contractor, the conduct of a suitability security investigation of an employee or contractor, or the grant, renewal, suspension, or revocation of a security clearance, to the extent that the information is relevant and necessary to the hiring agency's decision.

(b) Designated officers and employees of state or local (including the District of Columbia) law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.

(c) Members of a Presidential Transition Team for evaluating potential appointees.

(d) Security officials and investigators of Federal Government Agencies or Departments in connection with liaison or training purposes where appropriate during meetings, conferences, or training courses involving access to classified material.

(e) Federal, state, local, or private entities where appropriate for purposes of certification of security clearances of participants in training, conferences, meetings, facility visits, and other activities.

(f) In an appropriate proceeding before a court or administrative or regulatory body where the records are determined by the Department of Justice to be arguably relevant to the proceeding.

(g) The intelligence agencies of the Department of Defense, the National Security Agency, and the Central Intelligence Agency for use in intelligence activities.

(h) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, or tribal law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.

(i) An employee's designated representative in connection with the ARC appeals process.

(j) The news media and the public pursuant to 28 CFR 50.2 unless it is determined that of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(k) A Member of Congress or staff acting upon the Member's behalf when the Member requests the information on behalf of and at the request of the individual who is the subject of the record.

(l) The National Archives and Records Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(m) Contractors, grantees, experts, consultants, students, and others performing or working under a contract, service, grant, cooperative agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system of records.

(n) Former employees of the Department for purposes of: Responding to an official inquiry from a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee when such communications may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(o) An actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

(p) Federal, state, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

(q) Such recipients and under such circumstances and procedures as are mandated by statute or treaty.

Disclosure to consumer reporting agencies:

As stated in the "Categories of Records in the System," Item (4).

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Data is stored in electronic media via a configuration of personal computer, client/server mainframe systems architecture. Computerized records are maintained on hard disk, floppy diskettes, compact discs, magnetic tape, and/or optical disks. Paper files are stored as follows: (1) In a secure file room with controlled access; (2) locked file cabinets; and/or (3) other appropriate GSA approved security containers.

Retrievability:

Data is retrieved by searching under the individual's name, social security account number, or other identifier.

Safeguards:

Security measures include the use of safes, locked file cabinets, and/or restricted access space for manual records. Electronic records are safeguarded in accordance with DOJ policy and policy governing automated systems security and access. These safeguards include maintenance of technical equipment in restricted areas, and the required use of individual passwords and user identification codes to access the system.

Retention and disposal:

Records are retained and disposed of in accordance with items 22, 23, 24, and 25 of the General Records Schedule 18 as approved by the Archivist of the United States. Some records (such as Presidential Transition records) are retained only temporarily and then transferred to the appropriate agency.

System manager(s) and address:

System manager(s) and Addresses:

For records regarding former and current personnel and contractors employed by the Comptroller Boards, or Divisions (OBDs) as well as records regarding all Department attorneys, internal

honor program applicants, Schedule C personnel, non-career SES appointments, Presidential appointees, non-Departmental Federal Government personnel and ARC appeals for OE contact: Director, Security and Emergency Planning Staff, Attention: Assistant Director Personnel Security Group, Justice Management Division, U.S. Department of Justice, 2 Massachusetts Avenue, NW., Washington, DC 20530.

For records regarding former and current Bureau non-attorney personnel not specifically above and contractors, contact the individual Bureaus:

Security Programs Manager, Drug Enforcement Administration, 700 Army Navy Drive, Arlington, VA 22202.

Security Programs Manager, Federal Bureau of Prisons, 320 First Street, NW., Washington, DC 20543.

Security Programs Manager, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Ave., NW., Room 2240, Washington, DC 20226.

Security Programs Manager, Federal Bureau of Investigation, 935 Pennsylvania Avenue, Washington, DC 20535.

Security Programs Manager, United States Marshals Service, United States Marshals Service Headquarters, Washington, DC 20530-1000.

Security Programs Manager, Executive Office for U.S. Trustees, 20 Massachusetts Avenue, NW., Room 8202, Washington, DC 20530.

Security Programs Manager, National Drug Intelligence Center, 319 Washington Street, Johnstown, PA 15901.

Notification procedure:

Address inquiries to System Manager named above.

Record access procedures:

Record access procedures:

A request for access to a record from this system shall be made in writing to the System Manager, or in the case of the Federal Bureau of Prisons records, to the FOIA/PA Section 552, the envelope and the letter clearly marked "Privacy Act Request." The request should include a general description of the records sought and must include the requester's full name, current address, social security number, and date and place of birth. The request must be signed, dated, and either notarized or submitted under penalty of perjury. Some information may be exempt from access provisions as described in the section entitled "System Exempted from Certain Provisions of the Act." An individual who is the subject of a record in this system may request access to those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

Requests for copies of the investigative report should be directed to the appropriate investigative agency: the Office of Personnel Management at 1900 E St., NW., Room 5400, Washington, DC 20415; the Federal Bureau of Investigation at the address above, or to the appropriate investigative agency.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Record Access procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment, including tax return information. Some information may be exempt from contesting record procedures as described in the section entitled "Systems Exempted from Certain Provisions of the Act." An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

Record source categories:

Sources of information contained in this system are the individuals covered by the system, individuals and entities contacted by investigators, adjudicators, or other authorized personnel regarding individuals covered by the system, government records, and consumer report agencies.

System Exempted from certain provisions of the act:

The Attorney General has exempted this system from 5 U.S.C. 552a(c)(3) and (4); (d)(1)(3), and (4); (e)(1), (2), (3), (5) and (8); and (g). The exemptions will be applied only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j) & (k). A determination as to exemption shall be made at the time a request for access or amendment is received. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DOJ-007

System name:

Reasonable Accommodations for the Department of Justice (DOJ), JUSTICE/DOJ-007.

System location:

Records are maintained by designated Component Accommodation Coordinators in Department of Justice offices throughout the country. Records may be accessed by contacting the System Manager at the following address: U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530. (See Record Access Procedures below.)

Categories of individuals covered by the system:

Department of Justice employees and applicants who make requests for reasonable accommodation on the basis of a disability.

Categories of records in the system:

Records in this system include identifying information regarding persons requesting reasonable accommodations (e.g., requestor's name, title/series/grade, telephone number, date of request, e-mail address, office, description of accommodation requested, and reason for request) and the status of the response within the Department. Records in this system include: The original written request; the Department's response; the name, title and telephone number of office or staff members deciding or referring the matter; related letters/memo

copies of any enclosures/attachments, including medical records; the date an accommodation request was approved or denied; the reason a request was denied; the date an accommodation was provided; whether the recommended time frames were met as outlined in the Reasonable Accommodation Procedures; the reason the reasonable accommodation was needed; the type(s) of reasonable accommodation requested; the type(s) of accommodation provided; the source of technical assistance; whether medical or other appropriate support information was required to process the request, and if so, an explanation of why it was required; and other request-related information.

Authority for maintenance of the system:

The Rehabilitation Act of 1973, as amended, 29 U.S.C. 791; Executive Order 13164; Equal Employment Opportunity Commission's Policy Guidance on Executive Order 13164: Establishing Procedures to Facilitate the Provision of Reasonable Accommodation, Direct Transmittal Number 915.003, October 20, 2000.

Purpose(s):

The system documents and tracks requests made to the Department for reasonable accommodation, and action taken by the Department in response to the requests. It also serves as a reference source for inquiries and responses thereto on a "need to know" basis only. The Accommodation Coordinator(s) in each component of the Department will use the records to develop cumulative records, without individual identifiers, to track performance regarding the provision of reasonable accommodation by the Department.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Pursuant to subsection (b)(3) of the Privacy Act, information may be disclosed from this system as follows:

A. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

B. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of an individual who is the subject of the record.

C. To the General Services Administration and National Archives and Records Administration records management inspections conducted under the authority of 44 U.S.C. 2904 and

D. Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, to any civil or criminal law enforcement authority or appropriate agency, whether federal, state, local, foreign, or tribal, charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing a statute, rule, regulation, or order.

E. In an appropriate proceeding before a court, grand jury, or administrative or regulatory body when records are determined by DOJ to be arguably relevant to the proceeding.

F. To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

G. To a federal agency or entity that requires information relevant to a decision concerning hiring, appointment, or retention of an employee, the issuance of a security clearance, the conduct of a security or suitability investigation, or pursuit of other appropriate personnel matter.

H. To a federal, state, local, or tribal agency or entity that requires information relevant to a decision concerning the letting of a license or permit, the issuance of a grant or benefit, or other need for the information in performance of official duties.

I. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

J. To a former employee of the Department for purposes of: responding to an official inquiry from a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

K. To the White House (the President, Vice President, their staffs, and other entities of the Executive Office of the President (EOP)) for Executive Branch coordination of activities that relate to or have an effect upon the carrying out of the constitutional, statutory, or other or ceremonial duties of the President.

L. To such recipients and under such circumstances and procedures as are mandated by a federal statute or treaty.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are stored in paper files and may be entered into an electronic database in the

Retrievability:

Information can be retrieved by name of the individual making a request for reasonable accommodation; in the case of electronic databases, information may possibly be retrieved by other identifying search terms employed.

Safeguards:

Information in this system is safeguarded in accordance with applicable rules and policies, including the Department's automated systems security and access policies. In general, records and technical equipment are maintained in buildings with restricted access. The required use of password protection, identification features, and other system protection methods also restricts access to electronic information. Access is limited to those who have an official need for access to perform their official duties.

Retention and disposal:

Records are retained and disposed of in accordance with the Equal Employment Opportunity Commission's Policy Guidance on Executive Order 13164: Establishing Procedures to Facilitate the Provision of Reasonable Accommodation, Directives Transmittal Number 915.003, Circular 20, 2000. Records prepared by Accommodation Coordinators will be kept for a minimum

three years in accordance with General Records Schedule 1, Item 25g, as approved by National Archives and Records Administration. Records related to a particular individual accommodation request will be kept for the duration of the individual's employment. Any information that does not result in an appointment is kept in accordance with General R Schedule 1, Item 15. The records in this system are confidential and will be kept separate apart from the individual's personnel file.

System manager(s) and address:

Director, Equal Employment Opportunity Staff, Justice Management Division, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001.

Notification procedures:

Address inquiries to System Manager named above.

Record access procedures:

Requests for access must be in writing and should be addressed to the System Manager named above. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought, include the component where the records reside, if known (generally the employing component must include the requestor's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information include individuals who make written requests for reasonable accommodation, and supporting documentation from, for instance, rehabilitation counselors and Department decision makers (i.e., usually first line supervisors).

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/DOJ-008

System name:

Department of Justice Grievance Records, Justice/DOJ-008.

System location:

Records relating to grievances originating in a bureau (defined in 28 CFR 0.1) or an office, board, or division (defined in 28 CFR 0.1) are located in the central personnel or administrative office of the bureau, office, board, or division where the grievance originated, except for the Federal Bureau of Investigation (FBI), which is excluded from coverage under the Agency Grievance Procedure described in DOJ Order 1200.1, part 3, chapter 2.

Categories of individuals covered by the system:

Current or former Department of Justice employees, except for employees of the FBI, who submitted grievances under the Agency Grievance Procedure or in accordance with a negotiated grievance procedure.

Categories of records in the system:

The system contains records relating to grievances filed by Department employees under the Agency Grievance Procedure or under a negotiated grievance procedure. These case files contain all documents related to each grievance, including statements of witnesses, reports, interviews and hearings, factfinder's and/or arbitrator's findings and recommendations, copies of the original and final decision, and related correspondence and exhibits.

Authority for maintenance of the system:

5 U.S.C. 7121; 5 CFR part 771.

Purpose(s):

The records are maintained and used by the Department to resolve employee concerns working conditions, the administration of collective bargaining agreements, employee/supervisor relations, and work processes.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Based on a determination by the Department of Justice that such a need exists, these records and information in these records will be disclosed as follows:

- (1) To the appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the disclosing agency becomes aware of an indication of a violation or potential violation of criminal law or regulation;
- (2) To any source from which additional information is requested in the course of processing a grievance, to the extent necessary to identify the individual, inform the source of the purpose of the request, and identify the type of information requested;
- (3) To a Federal agency (or other establishment in the executive, legislative, and judicial branches of the Federal Government), in response to its request, in connection with the arrest or retention of an individual, the issuance of a security clearance, the conducting of a suitability or suitability investigation of an individual, the classifying of jobs, the letting of a contract, the issuance of a license, grant, or other benefit by the requesting agency, to the extent the information is relevant and necessary to the requesting agency's decision on the matter;
- (4) To a congressional office in response to an inquiry made at the request of the individual to whom the record pertains;
- (5) To the National Archives and Records Administration and the General Services Administration in records management inspections conducted under authority of 44 U.S.C. 2904 and 2906;
- (6) In an appropriate proceeding before a court, grand jury, or administrative or regulatory body.

when records are determined by DOJ, or the adjudicator, to be arguably relevant to the proceeding.

(7) To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery.

(8) To provide information to officials of labor organizations recognized under the Civil Service Reform Act when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting work conditions;

(9) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(10) To former employees of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(11) To specific entities when such disclosure is mandated by federal statute, treaty, or government-wide regulation.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

File folders and electronic storage.

Retrievability:

By the names of the individuals on whom the records are maintained.

Safeguards:

Lockable metal filing cabinets or a locked room, to which only authorized personnel have access; and appropriate safeguards for electronic storage.

Retention and disposal:

Disposed of four (4) years after closing of the case.

System manager(s) and address:

(a) Antitrust Division, Executive Officer, 601 D Street, NW., Rm. 10150, Washington, DC

(b) Civil Division, Director, Office of Administration, 1100 L Street, NW., Rm. 9018, Washington, DC 20530.

(c) Civil Rights Division, Executive Officer, 1425 New York Ave., NW., Rm. 5058, Washington, DC 20530.

(d) Criminal Division, Executive Officer, Office of Administration, 1400 New York Ave., NW., Rm. 5000, Washington, DC 20530.

(e) Environmental and Natural Resources Division, Executive Officer, 601 D Street, NW., Rm. 2038, Washington, DC 20004.

(f) Tax Division, Executive Officer, 601 D Street, NW., Rm. 7802, Washington, DC 20004.

(g) Drug Enforcement Administration, Deputy Assistant Administrator for Personnel, 700 Navy Drive, Rm. W3166, Arlington, VA 22202.

(h) Executive Office for Immigration Review, Office of the General Counsel, Employee/Labor Relations Unit, 5107 Leesburg Pike, Suite 2600, Falls Church, VA 22041.

(i) Executive Office for United States Attorneys, Office of Legal Counsel, 600 E Street, NW., Room 2200, Washington, DC 20530.

(j) Executive Office for United States Trustees, Human Resource Division, 20 Massachusetts Ave., NW., Rm. 8209, Washington, DC 20530.

(k) Federal Bureau of Prisons, Human Resource Management Division, Labor Manager Relations and Security Branch, 320 1st Street, NW., Bldg. 400, Washington, DC 20534.

(l) Office of Justice Programs, Office of Administration, Director, Office of Personnel, 810 1st Street, NW., Rm. 3330, Washington, DC 20531.

(m) United States Marshals Service, Assistant Director for Human Resources, 600 Army Drive, Suite 890, Arlington, VA 22202.

(n) Office of the Inspector General, Personnel Officer, 1425 New York Ave., NW., Suite 1000, Washington, DC 20530.

(o) Bureau of Alcohol, Tobacco, Firearms & Explosives, Personnel Division, Employee and Labor Relations Team, 650 Massachusetts Ave., NW., Rm. 4300, Washington, DC 20019.

(p) Other Offices, Boards, and Divisions: Director, Human Resources, Justice Management Division, 1331 Pennsylvania Ave., NW., Suite 1110, Washington, DC 20530.

Notification procedure:

It is required that individuals submitting grievances be provided a copy of the record upon grievance process. They may, however, contact the agency personnel or designated official where the action was processed, regarding the existence of such records on them. They must furnish the following information for their records to be located and identified: (1) Name, different, name at the time of the case, (2) date of birth, (3) approximate date of closing case and kind of action taken, (4) organizational component involved.

Record access procedures:

It is required that individuals submitting grievances be provided a copy of the record upon grievance process. However, after the action has been closed, an individual may request access to the official copy of the grievance file by contacting the personnel or designee of the bureau, office, board, or division where the action was processed (named above).

the caption "System Manager(s) and Addresses"). Individuals must provide the following information for their records to be located and identified: (1) Name, and if different, name at the time of the case, (2) date of birth, (3) approximate date of closing of the case and kind of action taken, (4) organizational component involved. Individuals requesting access must also follow the Department's Privacy Act regulations (28 CFR 16.41) regarding access to records and verification of identity.

Contesting record procedures:

Review of requests from individuals seeking amendment of their records which have been the subject of a judicial or quasi-judicial action will be limited in scope. Review of amendment requests of these records will be restricted to determining if the record accurately documents the action of the agency ruling on the case, and will not include a review of the merits of the action, determination, or finding.

Individuals wishing to request amendment to their records to correct factual errors should contact the personnel or designated office of the bureau, office, board or division where the grievance was processed (named above under the caption "System Manager(s) and Addresses"). Individuals must furnish the following information for their records to be located and identified: (1) Name, and if different, name at the time of the case, (2) date of birth, (3) approximate date of closing of the case and kind of action taken, (4) organizational component involved. Individuals requesting amendment must also follow the Department's Privacy Act regulations (28 CFR 16.41) regarding access and amendment to records and verification of identity.

Record source categories:

Information in this system of records is provided: (1) By the individual on whom the record is maintained, (2) by testimony of witnesses, (3) by agency officials, (4) from related correspondence from organizations or persons.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

JUSTICE/DOJ-009

System name:

Emergency Contact Systems for the Department of Justice, JUSTICE/DOJ-009.

System Locations:

U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530, and Department of Justice components and offices throughout the world.

Categories of individuals covered by the system:

Employees, former employees, and other individuals having business with the Department have provided contact information.

Categories of records in the system:

Home phone numbers, cellular phone numbers, pager numbers, numbers where individuals can be reached while on travel or otherwise away from the office, home addresses, email addresses, names and phone numbers of family members or other contacts, and contact information provided by individuals covered by this system of records to the Department.

Authority for maintenance of the system:

5 U.S.C. 301 and 44 U.S.C. 3101.

Purpose of the System:

To maintain contact information on employees and other individuals in case of emergency involving an employee or the Department, or when necessary for official purposes.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Pursuant to subsection (b)(3) of the Privacy Act, information may be disclosed from this

as follows:

A. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, an individual who is the subject of the record.

B. To the General Services Administration and National Archives and Records Administration records management inspections conducted under the authority of 44 U.S.C. 2904 and

C. Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, foreign, or tribal, law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.

D. In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator holds the records to be relevant to the proceeding.

E. To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

F. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

G. To a former employee of the Department for purposes of: responding to an official in a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

H. To the White House (the President, Vice President, their staffs, and other entities of the

Executive Office of the President (EOP)), and, during Presidential transitions, to the President Elect and Vice-President Elect and their designated transition team staff, for coordinative activities that relate to or have an effect upon the carrying out of the constitutional, statutory or other official or ceremonial duties of the President, President Elect, Vice-President, or Vice-President Elect.

I. To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Records are stored in electronic form and on paper.

Retrievability:

Information is retrieved by name of individual.

Safeguards:

Information in these systems is safeguarded in accordance with applicable rules and policies including the Department's automated systems security and access policies. In general, records and technical equipment are maintained in buildings with restricted access. The required use of password protection, identification features and other system protection methods also restrict access. Access is limited to those who have an official need for access to perform their official duties.

Retention and disposal:

Records about individuals who are not current Department employees are retained until no longer needed, pending approval by the National Archives and Records Administration (115); other records are retained and disposed of in accordance with General Records Schedule 1, item 6.

System manager and Address:

Deputy Assistant Attorney General, Policy, Management and Planning, MAIN Justice Bu
950 Pennsylvania Ave., NW., Washington, DC 20530

Notification Procedures:

Address inquiries to System Manager named above.

Record access procedures:

Requests for access must be in writing and should be addressed to the System Manager named above. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Records Access procedures and to the System Manager named above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in these systems include employees and other individuals covered by this system, and the Federal Government.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/DOJ-010

System name:

Leave Sharing Systems, JUSTICE/DOJ-010.

Security classification:

Not classified.

SYSTEM LOCATIONS:

Systems are maintained by designated Leave Transfer Coordinators throughout the Department of Justice (DOJ), Human Resources Offices, with the exception of the Leave Coordinator, whose system is located at the following address: U.S. Department of Justice Management Division, 1331 Pennsylvania Ave., NW., Suite 1110, Washington, DC 20530. The Leave Transfer Coordinators' system location is shown in this notice under the Systems Managers and Addresses.

Categories of individuals covered by the system:

Individuals covered by the Voluntary Leave Transfer Program (VLTP) are current employees (recipients and donors) of the DOJ, and employees in other Federal agencies who make voluntary leave donations to or receive voluntary leave donations from DOJ employees, excluding employees of the Federal Bureau of Investigations (FBI), Central Intelligence Agency, Defense Intelligence Agency, National Security Agency or any other Executive branch or unit thereof, as determined by the President, whose principal function is the conduct of foreign intelligence or counterintelligence activities.

Individuals covered by the Voluntary Leave Bank Program (VLBP) are current employees of the DOJ, excluding the FBI and Executive Office for U.S. Trustees.

Categories of records in the system:

Records maintained in the Voluntary Leave Transfer (VLT) system include two categories of records: Recipient records—VLT Recipient application, medical records, time and attendance report, and related comments; and Donor records—Authorization to Transfer Leave application, time and attendance report, and related comments.

Records maintained in the Voluntary Leave Bank (VLB) system include two categories of

records: Recipient records—VLB Recipient application, medical records, time and attendance report, and related comments; and Donor records—Request for Leave or Approved Absence (SF-71), time and attendance report, and related comments.

Authority for maintenance of the system:

Title 5, United States Code, Chapter 63, Subchapter III; 5 United States Code, Part 630 Subpart I and J; Public Law 103-103, the Federal Employees Leave Sharing Amendments Act of 1993.

PURPOSE OF THE SYSTEM:

The Voluntary Leave Transfer and Leave Bank systems record and track donor and recipient leave or medical records to assist employees without available paid leave with medical emergencies that require an absence from duty. The VLTP covers employees who experience medical emergencies, as well as employees who are caring for family members who are experiencing medical emergencies. The VLBP works in conjunction with the existing VLTP at the Department. The Leave Bank accepts membership contributions of annual leave, and makes that leave available to qualified members who experience medical emergencies.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Pursuant to subsection (b) (3) of the Privacy Act, information may be disclosed from this system as follows:

- A. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf and at the request of an individual who is the subject of the record.
- B. To the National Archives and Records Administration in records management inspection conducted under the authority of 44 U.S.C. 2904 and 2906.
- C. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the DOJ determines that the records are arguably relevant to the proceeding or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator holds the records to be relevant to the proceeding.

D. To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion on such matters as settlements, plea bargaining, or informal discovery proceedings.

E. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or records.

F. To designated timekeepers to adjust employees' leave balances.

G. To designated Leave Bank Board members to administer donated leave, review reciprocal applications, and make decisions on appeals.

H. To the Office of Personnel Management to evaluate the effectiveness of the program

I. Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, foreign, or tribal, law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.

J. To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

K. The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Disclosure to consumer reporting agencies:

Not Applicable.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:***Storage:***

Applications and medical records are stored in paper files. Time and attendance records are stored in an automated system. Paper files are stored in secured areas.

Retrievability:

Information is retrieved by employee name, Social Security number, or report generated by the automated system.

Safeguards:

Safeguard measures include the use of secured areas, user identification and password, restricted access to data, and envelopes which appropriately identify the sensitive nature of the enclosed information.

Retention and disposal:

Records are retained and disposed of in accordance with the General Records Schedule for Civilian Personnel Records. They are destroyed one year after the end of the year in which the file is closed.

System manager(s) and address:

Leave Bank System Manager: Director, Personnel Staff, Justice Management Division, 1000 Pennsylvania Ave., NW, Suite 1110, Washington, DC 20530.

Leave Transfer System Managers:

Leave Transfer Coordinator:

Antitrust Division, Executive Officer, 601 D Street, NW, Rm. 10150, Washington, DC

Civil Division, Director, Office of Administration, 1100 L Street, NW, Rm. 9018, Washington, DC 20530

Civil Rights Division, Executive Officer, 1425 New York Ave., NW, Rm. 5058, Washington, DC 20530

Criminal Division, Executive Officer, Office of Administration, 1400 New York Ave., NW, Rm. 5000, Washington, DC 20530

Environmental and Natural Resources Division, Executive Officer, 601 D Street, NW, Rm. 2038, Washington, DC 20004

Tax Division, Executive Officer, 601 D Street, NW, Rm. 7802, Washington, DC 20004

Drug Enforcement Administration, Deputy Assistant Administrator for Personnel, 70 Navy Drive, Rm. W3166, Arlington, VA 22202

Executive Office for Immigration Review, Office of the General Counsel, Employee and Labor Relations Unit, 5107 Leesburg Pike, Suite 2400, Falls Church, VA 22041

Executive Office for United States Attorneys, Personnel Staff, 600 E Street, NW, Room 3000, Washington, DC 20530

Executive Office for United States Trustees, Human Resource Division, 20 Massachusetts Ave., NW, Rm. 8209, Washington, DC 20530

Federal Bureau of Prisons, Human Resource Management Division, Labor Management Relations and Security Branch, 320 1st Street, NW, Bldg. 400, Washington, DC 20534

Office of Justice Programs, Office of Administration, Director, Office of Personnel, 800 1st Street, NW, Rm. 3330, Washington, DC 20531

United States Marshals Service Headquarters, Washington, DC 20530-1000

Office of the Inspector General, Personnel Officer, 1425 New York Ave., NW, Suite 700, Washington, DC 20530

Bureau of Alcohol, Tobacco, Firearms and Explosives, Personnel Division, Employee Labor Relations Team, 650 Massachusetts Ave., NW, Rm. 4300, Washington, DC 200

Other Offices, Boards, and Divisions: Director, Human Resources, Justice Management Division, 1331 Pennsylvania Ave., NW, Suite 1110, Washington, DC 20530

Notification procedure:

Address inquiries to System Managers named above.

Record access procedures:

Requests for access to records from the system must be in writing to the System Manager be clearly marked "Privacy Act Access Request." The request should include the component where the records reside, if known (generally, the employing component), and must include the requestor's name, title, organization, address, phone number and a general description and purpose of records sought, and must include the requestor's full name, current address and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. Records will be released in accordance with the Freedom of Information Act, as well as the Privacy Act.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Please include the information requested in "Record Access Procedures" above.

Record source categories:

Sources of information include employees who make written requests for application to leave sharing programs, including supporting documentation, such as time and attendance records and medical records.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[\[TOP\]](#)

JUSTICE/DOJ-011

System name:

Access Control System (ACS).

System location:

Records are located at the Department of Justice (DOJ) Robert F. Kennedy Main Justice Building (MJB), 950 Pennsylvania Ave., NW., Washington, DC 20530, and at other buildings with DOJ-controlled access.

Categories of individuals covered by the system:

Individuals who have applied for, sought, been considered for, attempted and/or obtained access to the MJB and other buildings, office space, or real property with DOJ-controlled access control systems. May include: current and former DOJ employees, contractors, vendors, grantees, experts, consultants, task force personnel, volunteers, detailees, visitors and other non-DOJ employees. May also include persons identified as employers, sponsors, references, or contacts for the above individuals.

Categories of records in the system:

Records may include: names; social security numbers; dates of birth; physical descriptions; badge numbers; information on employer, sponsor, contacts, and/or references; home and business addresses and phone numbers; dates and times of entry, exit, and/or passage through control points; signatures, photographs, videos, electronic images, fingerprints, other biometric identifiers; vehicle identification data; drivers license number; purpose of visit and person visited and/or other related information.

Authority for maintenance of the system:

Executive Order 12958, as amended by Executive Order 13292; Title 5 U.S.C. 552a(e)(1)

44 U.S.C. chapters 21 and 33. These statutes and Executive Orders are directed toward security of United States Government records maintained by federal agencies. Title 40 U.S.C. chapter 318a; and Title 41 CFR section 102–81.10 and 81.15. This statute and the federal regulations are directed toward security of United States Government buildings and the contents therein.

Purpose(s):

Records in this system are necessary to maintain the security of the personnel and locations which the DOJ operates, and of DOJ records, vehicles, property and equipment, and are used to determine eligibility and/or the status of individuals who have applied for, sought, been considered for, attempted and/or obtained access to such locations. Records in this system are also used to maintain control of badges issued for access to locations where the DOJ operates.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records or information from this system of records may be disclosed under the following circumstances when it has been determined by the Department of Justice that such a disclosure exists:

To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that disclosure of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

To a Member of Congress or staff acting upon the Member's behalf when the Member requests the information on behalf of and at the request of the individual who is the subject of the record.

To the National Archives and Records Administration in records management inspection or audit conducted under the authority of 44 U.S.C. 2904 and 2906.

To any criminal, civil, or regulatory law enforcement authority (whether federal, state, local, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

To a governmental entity lawfully engaged in collecting law enforcement, law enforcement

intelligence, or national security intelligence information for such purposes.

To any person or entity in either the public or private sector, domestic or foreign, if deemed by the DOJ to be necessary in eliciting information or cooperation from the recipient for use by the DOJ in furthering the purposes of the system, e.g., disclosure of personal identifying information to an associate or employer of a person to confirm the person's identity, suit and reason for access to a DOJ facility.

In an appropriate proceeding before a court, or administrative or adjudicative body, where the Department of Justice determines that the records are arguably relevant to the proceeding in an appropriate proceeding before an administrative or adjudicative body when the adjudicator holds the records to be relevant to the proceeding.

To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit.

To federal, state, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or

To contractors, grantees, experts, consultants, students, and others performing or working under a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee where such may be necessary for personnel-related or other official purposes where the Department

requires information and/or consultation assistance from the former employee regarding matter within that person's former area of responsibility.

Disclosure to consumer reporting agencies:

Not applicable.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Most information is maintained in computerized form and stored in memory, on disk storage, computer tape, or other computer media. However, some information may also be maintained in hard copy (paper) or other form.

Retrievability:

Information is typically retrieved by name of the individual, other personal identifiers, or access badge number.

Safeguards:

Records in this system are maintained in limited access space in DOJ-controlled facilities and offices. Computerized data is password protected. All DOJ personnel are required to pass background investigation. The information is accessed only by authorized DOJ personnel. Non-DOJ personnel properly authorized to assist in the conduct of an agency function may have access to these records.

Retention and disposal:

Records in this system in all formats are maintained and disposed of in accordance with the appropriate authority of the National Archives and Records Administration.

System manager AND ADDRESS:

For the Main Justice Building and certain satellite offices in the Washington DC Metropolitan Area.

Area: Director, Security and Emergency Planning Staff, Justice Management Division, F 6217, 950 Pennsylvania Ave., NW., Washington, DC 20530.

For other Specific Buildings/Components:

Security System Manager, Justice Data Center—Washington, 1151–D Seven Locks Rd. Rockville, MD 20854;

Security System Manager, Justice Data Center—Dallas, 207 S. Houston St., Dallas, TX

Chief, Physical Security, Executive Office of U.S. Attorneys, U.S. DOJ.EOUSA–SPS, 60 Street, NW., Suite 2600, Washington, DC 20530;

Director, Security Programs Staff, Criminal Division, 1331 F Street, NW., Suite 300, Washington, DC 20530;

Deputy Chief Inspector, Office of Security Programs, Drug Enforcement Administration, Army Navy Drive, Arlington, VA 22202;

Chief, Security and Emergency Programs Division, Bureau of Alcohol, Tobacco, Firearm Explosives, 650 Massachusetts Avenue, NW., Room 2240, Washington, DC 20226;

Security Program Manager, Office of the Inspector General, 950 Pennsylvania Ave., NW Washington, DC 20530;

Security Programs Manager, Office of Intelligence Policy and Review, Department of Justice, Washington, DC 20530;

Security Programs Manager, Executive Office for Immigration Review, 5107 Leesburg Pike, Suite 2103, Falls Church, VA 22041;

Case Management Specialist, Office of the United States Trustee, 33 Whitehall St., 21st Floor, New York, NY 10004–2112;

Security Programs Manager, United States Marshals Service, United States Marshals Service Headquarters, Washington, DC 20530–1000;

DOJ/INTERPOL-USNCB, 1301 New York Ave., NW., Washington, DC 20530;

Security Program Manager, Tax Division, 555 Fourth St., NW., Washington, DC 20530;

Chief, Office of Security and Classified Programs, National Drug Intelligence Center, 31 Washington St., Johnstown, PA 15901;

NOTIFICATION PROCEDURES:

Same as Record Access Procedures.

Record access procedures:

A request for access to a record from the system shall be made in writing with the envelope and the letter clearly marked "Privacy Act Request." Include in the request your full name and complete address. The requester must sign the request; and, to verify it, the signature must be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury and dated as a substitute for notarization. You may submit any other identifying data you wish to furnish to assist in making a proper search of the system. Requests for access should be addressed to: Facilities and Personnel Group, Security and Emergency Planning Staff, Justice Management Division, Room 6217, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should always direct their request to the appropriate System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Include information requested above for Record Access Procedures.

Record source categories:

See Categories of Individuals Covered by the System.

EXEMPTIONS CLAIMED BY THE SYSTEM:

None.

[\[TOP\]](#)

JUSTICE-012

System name:

Department of Justice Regional Data Exchange System (RDEX)

Security classification:

Unclassified.

System location:

United States Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001, and other Department of Justice offices throughout the country.

Categories of individuals covered by the system:

Individuals covered by this system include individuals who are referred to in potential or cases or matters of concern to the Federal Bureau of Prisons (BOP), the United States Marshals Service (USMS), the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), and as individuals referred to in law enforcement information contributed by certain state and local law enforcement agencies that participate in the RDEX system under memoranda of understanding with the Department of Justice. Because the system contains audit logs regarding queries, individuals who use the system to conduct such queries are also covered.

Categories of records in the system:

The system consists of unclassified criminal law enforcement records collected and provided by the BOP, the USMS, the ATF, the DEA, the FBI, and certain state and local law enforcement agencies, including: investigative reports and witness interviews from both open and closed cases; criminal event data (e.g., characteristics of criminal activities and incidents that identify links or patterns); criminal history information (e.g., history of arrests, nature

disposition of criminal charges, sentencing, confinement, and release); and identifying information about criminal offenders (e.g., name, address, date of birth, birthplace, physical description). The system also consists of audit logs that contain information regarding queries made of the system.

Authority for maintenance of the system:

The system was established and is maintained pursuant to 28 U.S.C. 533 and 534; Presidential Decision Directives 39 and 62; and Executive Order 13,356.

PURPOSE OF THE SYSTEM:

This system is maintained for the purpose of ensuring that Department of Justice criminal enforcement information is available for users at all levels of government so that they can effectively investigate, disrupt, and deter criminal activity, including terrorism, and protect national security. RDEX furthers this purpose by consolidating certain law enforcement information from other Department of Justice systems, as well as certain state and local enforcement information, in order that it may more readily be available for sharing with other law enforcement entities.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information may be disclosed from this system as follows:

- (1) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.
- (2) To a governmental entity lawfully engaged in collecting criminal law enforcement, criminal law enforcement intelligence, or national security intelligence information for law enforcement or intelligence purposes.
- (3) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

(4) In an appropriate proceeding before a court, or administrative or adjudicative body, or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(5) To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings.

(6) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(7) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(8) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(9) To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

(10) To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

(11) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

(12) To any person or entity if deemed by the Department to be necessary in order to elicit information or cooperation from the recipient for use by the Department in the performance of its duties.

an authorized law enforcement activity.

(13) To any individual, organization, or governmental entity in order to notify them of a terrorist threat for the purpose of guarding against or responding to such a threat.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system: Storage:

Records in this system are stored primarily in electronic form. However, some information also be stored in paper form.

Retrievability:

Records are retrieved by the name and/or other identifier(s) of the individual.

Safeguards:

Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including the Department's automated systems security and access policies. Records and technical equipment are maintained in buildings with restricted access. Passwords, password protection identification features, and other system protection methods also restrict access to information in this system. Only Department of Justice personnel and other users who are members of law enforcement agencies, have undergone background and criminal history checks, and have received appropriate training will be permitted access to the system and such access is limited to those who have an official need for access in order to perform their duties.

Retention and disposal:

Records in this system are maintained and disposed of in accordance with all applicable statutory and regulatory requirements.

System managers and Addresses:

For the RDEX system generally and for state and local information: Director, Federal Bureau of Investigation, 935 Pennsylvania Avenue, NW., Washington, DC 20535.

For ATF information: Associate Director, Office of Strategic Intelligence and Information, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW Washington, DC 20226.

For BOP information: Assistant Director, Correctional Programs Division, Federal Bureau of Prisons, 320 First Street, NW., Washington, DC 20534.

For DEA information: Assistant Administrator, Operations Division, Drug Enforcement Administration, Freedom of Information Section, Washington, DC 20537.

For FBI information: Director, Federal Bureau of Investigation, 935 Pennsylvania Avenue, NW Washington, DC 20535.

For USMS information: Assistant Director, Investigative Services Division, United States Marshals Service, Washington, DC 20530–1000.

Notification Procedures:

Same as Record Access Procedures.

Record access procedures:

Requests for access may be made by appearing in person or by writing to the appropriate system manager at the address indicated in the System Managers and Addresses section above. The envelope and letter should be clearly marked "Privacy Act Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and notarized or submitted under penalty of perjury. Some information may be exempt from disclosure as described in the section entitled "Exemptions Claimed for the System." An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination of whether a record may be accessed will be made after a request is received.

Although no specific form is required, forms may be obtained for this purpose from the FOIA/PA Mail Referral Unit, Justice Management Division, United States Department of 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001, or on the Department of Web site at <http://www.usdoj.gov/04foia/att—d.htm>.

Contesting record procedures:

Individuals seeking to contest or amend information maintained in the system should direct their requests to the appropriate system manager at the address indicated in the System Managers and Addresses section, above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information may be exempt from contesting record procedures as described in the section entitled "Exemptions Claimed for the System." An individual who is the subject of a record in this system may seek amendment of any records that are not exempt. A determination of whether a record is exempt from amendment will be made after a request is received.

Record source categories:

Records in RDEX come directly from the criminal law enforcement files and records systems of the participating Department of Justice components (ATF, BOP, DEA, FBI, and USMS), as well as certain state and local law enforcement agencies participating in the RDEX system under memoranda of understanding with the Department of Justice.

Exemptions Claimed for the System:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d)(1), (2), (3), (5), and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a. These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e), and are published in today's *Federal Register*.

[\[TOP\]](#)

System Name:

Justice Federal Docket Management System (Justice FDMS).

Security Classification:

None.

System Location:

U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530 and c
Department of Justice offices.

Categories of Individuals Covered by the System:

Any person—including private individuals, representatives of Federal, State or local governments, businesses, and industries, that provides personally identifiable information pertaining to DOJ and persons mentioned or identified in the body of a comment.

Categories of Records in the System:

Agency rulemaking material includes but is not limited to public comments received through FDMS pertaining to DOJ rulemaking where such comments contain personally identifiable information; and any other supporting rulemaking documentation.

Authority for Maintenance of the System:

Section 206(d) of the E-Government Act of 2002 (Pub. L. 107–347, 44 U.S.C. Chapter 3

Purpose(s):

To assist the Federal Government in allowing the public to search, view, download, and comment on Federal agency rulemaking documents in one central on-line location and contact commenters if necessary.

Routine Uses of Records Maintained in the System Including Categories of Users and Purposes of Such Uses:

A. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

B. To appropriate officials and employees of a Federal agency or entity that requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

C. To Federal, State, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

D. Information may be disclosed to the Office of Management and Budget at any stage in the legislative coordination and clearance process in connection with private relief legislation set forth in OMB Circular No. A-19, Circular No. A-130, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals.

E. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the records.

F. In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding, or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

G. To the National Archives and Records Administration (NARA) for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

H. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or

records.

I. To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings.

J. To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

K. To a former employee of the Department for purposes of: responding to an official inquiry of a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

L. To such recipients and under such circumstances and procedures as are mandated by a Federal statute or treaty.

M. To the White House (the President, Vice-President, their staffs, and other entities of the Executive Office of the President), and, during Presidential transitions, to the President-elect and Vice-President Elect and their designated transition team staff, for coordination of activities that relate to or have an effect upon the carrying out of the constitutional, statutory, or ceremonial duties of the President, President-elect, Vice-President or Vice-President-elect.

N. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to Consumer Reporting Agencies:

Not Applicable.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing Records in the System:***Storage:***

Records will be maintained in computer databases compliant with DOD 5015.2 electronic records standards. A paper copy of all rulemaking docket materials will also be maintained in the components and constitutes the official record.

Retrievability:

The FDMS will have the ability to retrieve records by various data elements and keyword searches, including: Name, Agency, Component, Docket Type, Docket Sub-Type, Agency Docket ID, Docket Title, Docket Category, Document Type, CFR Part, Date Comment Received, and *Federal Register* Published Date.

Safeguards:

Justice FDMS security protocols will meet multiple NIST Security Standards from Authentication to Certification and Accreditation. Records in the Justice FDMS will be maintained in a secure, password protected electronic system that will utilize security hardware and software to include: multiple firewalls, active intruder detection, and role-based access controls. Additional safeguards will vary by component.

Retention and Disposal:

Each component will handle its records in accordance with its records schedule as approved by the National Archives and Records Administration (NARA). Electronic data will be retained and disposed of in accordance with the component's records schedule pending approval from the NARA. The majority of documents residing on this system will be public comments and other documentation in support of Federal rulemakings. All *Federal Register* rulemaking documents are part of the Justice FDMS and are identified as official records and retained by NARA.

System Managers and Addresses:

Technical Issues: Justice Department, Deputy Chief Information Officer for E-Government, Office of the Chief Information Officer, United States Department of Justice, 950 Pennsylvania Avenue, NW., RFK Main Building, Washington, DC 20530.

Policy Issues: Justice Department FDMS Policies System Administrator, Office of Legal Policy, United States Department of Justice, 950 Pennsylvania Avenue, NW., RFK Main Building, Washington, DC 20530.

Component Managers can be contacted through the Department's System Managers.

Notification Procedure:

Records concerning comments received through FDMS pertaining to DOJ rulemaking are maintained by the individual DOJ component to which the comment was directed. Inquiries regarding these records should be addressed to the particular DOJ component maintaining the records at Department of Justice, 950 Pennsylvania Avenue, NW., RFK Main Building, Washington, DC 20530. For records concerning the DOJ FDMS system generally, inquiries should be made to the System Manager for technical or policy issues as appropriate, listed above.

Record Access Procedures:

Requests for access may be made by appearing in person or by writing to the appropriate system manager at the address indicated in the System Managers and Addresses section as described in the Notification Procedures, above. The envelope and letter should be clearly marked "Privacy Act Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed, dated, and either notarized or submitted under penalty of perjury. Although no specific form is required, forms may be obtained for this purpose from the FOIA/PA Mail Referral Unit, Justice Management Division, United States Department of Justice, 950 Pennsylvania Avenue, NW., Washington DC 20530-0001, or on the Department of Justice Web site at http://www.usdoj.gov/04foia/att_d.htm.

Contesting Records Procedures:

Individuals seeking to contest or amend information maintained in the system should direct their requests to the appropriate system manager at the address indicated in the System Managers and Addresses section, or as described in the Notification Procedures, above, stating clearly and concisely what information is being contested, the reasons for contesting, and the proposed amendment to the information sought.

Record Source Categories:

Any person, including public citizens and representatives of Federal, state or local governments; businesses; and industries.

Exemptions Claimed for the System:

None.

[\[TOP\]](#)

JUSTICE/DOJ-014

SYSTEM NAME:

Employee Directory Systems for the Department of Justice

SECURITY CLASSIFICATION:

Sensitive But Unclassified Information and/or Controlled Unclassified Information

SYSTEM LOCATION:

United States Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001, and other Department of Justice offices throughout the United States and

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Employees, former employees, detailees, student aides, law clerks, volunteers, contractors and other personnel employed by or otherwise affiliated with the Department.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records maintained on the internal Departmental email directory system may include name, position title, office location, office telephone and facsimile numbers, office address, and electronic mail (e-mail) address.

Records maintained by component directory systems may include name, position title, office location, office telephone and facsimile numbers, office address, electronic mail (e-mail) address, as well as certain limited voluntarily submitted information including photographs, professional background records (such as law school name and year of graduation, clerical bar memberships, advanced degrees earned, foreign language expertise, and notary public commission). In addition, some directories may include certain information to which access is restricted to users depending on the roles and responsibilities within the system. Specifically, some directories may include information collected for a specific statutory or management purpose and may include limited relevant professional background information. Some component directories may also include emergency contact information, which may be used to contact the individual named, or his/her authorized designee, in the event of an emergency during or outside of official duty hours. Emergency contact information maintained in component directories may include home addresses and telephone numbers; cellular telephone numbers; pager numbers; other alternate telephone numbers where individuals or their designees may be reached while away on travel, assigned work detail, or other extended absence from the office; email addresses; names, telephone numbers and email addresses of family members or other emergency contacts; and other contact information individuals wish to provide. [Note: The Department has provided notice for emergency contact information not maintained in component employee directories in Department of Justice –009 “Emergency Contact Systems for the Department of Justice,” 69 FR 1762 (Jan. 12, 2004).]

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority to establish and maintain this system is contained in 5 U.S.C. 301 and 44 U.S.C. 3101, which authorize the Attorney General to create and maintain federal records of agency activities, as well as other specific statutory authorities that authorize the maintenance of records by the Department of Justice.

PURPOSE(S):

To allow Department personnel to collaborate within each individual component and with

Department and to facilitate professional contacts in order to perform their duties and to the Department's business practices.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

(a) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

(b) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

(c) To the National Archives and Records Administration in connection with records retention and disposition issues and for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(d) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(e) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, territorial, tribal, or foreign law enforcement authority, or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

(f) To appropriate agencies, entities, and persons when: (1) The Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (with

maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonable and necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(g) To appropriate officials and employees of a federal agency or entity when the information is relevant to a decision concerning the hiring, appointment, or retention of an employee; the assignment, detail, or deployment of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

(h) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(i) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings.

(j) To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

(k) To the news media and the public, including disclosures pursuant to 28 CFR § 50.2, when it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system are stored on paper and/or in electronic form. Records are stored

accordance with applicable executive orders, statutes, and agency implementing recommendations.

RETRIEVABILITY:

Information is retrieved by the individual's name, and in some instances, email address.

SAFEGUARDS:

Information in this system is safeguarded in accordance with appropriate laws, rules, and policies, including the Department's automated systems security and access policies, and access to such information is limited to Department personnel, contractors, and other authorized personnel who have an official need for access in order to perform their duties. Access to electronic employee directory systems is restricted to Department personnel, contractors, and other affiliated persons with accounts on the Department's computer network because it is accessed via the Department's intranet or the specific component's intranet. Additionally, access to certain information in directories maintained by components is restricted to certain users depending on their roles and responsibilities within that system. For example, access to emergency contact information that is maintained in some component's directories is strictly limited to managers and personnel with a need to know in order to contact a designee in the event of an emergency.

RETENTION AND DISPOSAL:

Records are retained during their useful life in accordance with records retention schedules approved by the National Archives and Records Administration.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Office of Privacy and Civil Liberties, Department of Justice, National Place Building
1331 Pennsylvania Avenue, NW., Suite 940, Washington, DC 20530.

NOTIFICATION PROCEDURE:

Same as record access procedures.

RECORD ACCESS PROCEDURES:

Access to employee directory systems is restricted to Department employees, contractors and other affiliated persons with accounts on the Department's computer network because they are accessed via the Department's intranet or the specific component's intranet. Additionally, access to certain information in component directories is restricted to users depending on their roles and responsibilities within that system. For example, access to the emergency contact information included in some component directories is restricted to those managers and personnel who need to know the information in order to contact a designee in the event of an emergency.

For access to Departmental e-mail system information, individuals may directly access information through the Department's internal e-mail system.

For certain component employee directory systems, individuals may directly or through a system administrator, post, verify, correct, and/or remove information in their individual employee profiles.

All other requests for access may be made by writing to the System Manager named at the end of the envelope. The envelope and letter should be clearly marked "Privacy Act Request." The request should include a general description of the records sought and must include the requester's full name, current address, and place and date of birth. The request must be signed and either notarized or submitted under penalty of perjury. A determination of whether a record may be accessed will be made after a request is received.

Although no specific form is required, you may obtain forms for this purpose from the Freedom of Information Mail Referral Unit, Justice Management Division, United States Department of Justice, 900 Pennsylvania Avenue, NW., Washington, DC 20530-0001, or on the Department of Justice Web site at http://www.usdoj.gov/04foia/att_d.htm.

CONTESTING RECORD PROCEDURES:

For information maintained in the internal Departmental e-mail system, individuals may contact a system administrator to inquire about updating, correcting, and/or removing information.

For certain component employee directory systems, individual employees may directly or through a system administrator, post, verify, correct, and/or remove information in their individual employee profiles.

Individuals may also contest or amend information maintained in the system by directing requests to the appropriate component system administrator or the System Manager named above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. A determination whether a record may be contested or amended will be made after a request is received.

RECORD SOURCE CATEGORIES:

Sources of information contained in this system are from existing Department and/or component employee directory information, as well as employees, student aides, law clerks and volunteers, contractors, and other associated personnel who provide such information.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[\[TOP\]](#)

Bureau of Alcohol Tobacco, Firearms, and Explosives

JUSTICE/ATF-001

System name:

Administrative Record System-Justice/ATF-001.

System location:

Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), 650 Massachusetts Avenue, Washington, DC 20226. Components of this record system are geographically dispersed throughout the Bureau's field offices. A list of field offices is available by writing to the Civil Liberties Disclosure Division, Room 8400, 650 Massachusetts Avenue, NW., Washington, DC 20535.

Categories of individuals covered by the system:

(1) Present employees of the Bureau of ATF. (2) Former employees of the Bureau of ATF. (3) Claimants against the Bureau of ATF.

Categories of records in the system:

Documents related to claims submitted including: (1) Accident Report—vehicle; (2) Fatal reports; (3) Injury reports; (4) Chief Counsel and District Counsel memoranda and opinions.

Authority for maintenance of the system:

(1) Federal Claims Collection Act. (2) Federal Property and Administration Services Act as amended. (3) Federal Tort Claims Act. (4) Military Personnel and Civilian Claims Act. (5) Occupational Safety and Health Act of 1970. (6) Small Claims Act. (7) 5 U.S.C. 1302, 3302.

Purpose(s):

The purpose of this system is to resolve claims submitted to the Bureau of Alcohol, Tobacco, Firearms and Explosives.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record in this system may be disclosed as a routine use:

A. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

B. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system's records.

C. In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, or tribal law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.

D. To officials and employees of a federal agency or entity, including the White House, requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance of a security clearance; the execution of a security or suitability investigation; the classification of a job; or the issuance of a grant or benefit.

E. In an appropriate proceeding before a court or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding.

F. To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

G. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

H. To federal, state, and local licensing agencies or associations, which require information concerning the suitability or eligibility of an individual for a license or permit.

I. To the General Services Administration and National Archives and Records Administration records management inspections conducted under the authority of 44 U.S.C. 2904 and

J. To a former employee of the Department for purposes of: responding to an official inquiry from a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

K. To such recipients and under such circumstances and procedures as are mandated by a federal statute or treaty.

L. To an organization or individual in either the public or private sector where there is reason to believe the recipient is or could become the target of a particular criminal activity or conspiracy to the extent the information is relevant to the protection of life or property.

M. To individuals and organizations to the extent necessary to obtain relevant information needed by the Bureau to render a decision in regard to an administrative matter.

N. To Treasury Department, Alcohol and Tobacco Tax and Trade Bureau employees, where necessary to accomplish a Treasury Department or Department of Justice function relating to this system of records.

O. To unions recognized as exclusive bargaining representatives in accordance with procedures contained in the Civil Service Reform Act of 1978, 5 U.S.C. 7111 and 7114.

P. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Active records are stored in file folders in security filing cabinets. Inactive records are stored in file folders at Federal Records Centers. Records are also stored in electronic media.

Retrievability:

Records are retrieved by name of individual.

Safeguards:

Direct access is restricted to personnel in the Department of Justice in the performance of their duty. Records are transmitted to routine users on a need to know basis or where a right of access is established, and to others upon verification of the substance and propriety of request. These records are stored in lockable metal file cabinets in rooms locked during non-duty hours. The records stored in electronic media are password protected.

Retention and disposal:

Records are retained in accordance with General Records Schedules Numbers 1 through 5.

issued by the National Archives and Records Administration, and Bureau of Alcohol, Tobacco, Firearms and Explosives records control schedules numbers 101 and 201 and disposed by shredding or burning.

System manager(s) and address:

Assistant Director, Office of Management/Chief Financial Officer, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW., Washington, DC 20226.

Notification procedure:

See "Record access procedures" below.

Record access procedures:

For records accessible through the Privacy Act, a request should be made in writing and mailed to the Disclosure Division, Privacy Act Request, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW., Washington, DC 20226. The envelope and the letter should be clearly marked "Privacy Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed, dated, and either notarized or submitted under penalty of perjury.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Record Access procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment, including tax return information.

Record source categories:

(1) Administrative records; (2) Claimants; (3) Doctors; (4) Employee records; (5) Fiscal records; (6) Former employees of the Bureau of ATF; (7) Former employers; (8) General Service Administration; (9) Individuals who have information relevant to claims; (10) Inspections records; (11) Internal Investigation reports; (12) Police reports; (13) Present employees

Bureau of ATF; (14) Supervisors; (15) Witnesses; (16) Insurance companies.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

JUSTICE/ATF-003

System name:

Criminal Investigation Report System, Justice/ATF-003.

System location:

Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW Washington, DC 20226. Components of this record system are geographically disperse throughout Bureau of Alcohol, Tobacco, Firearms and Explosives' field offices. A list of offices is available by writing to the Chief, Disclosure Division, Room 8400, 650 Massachusetts Avenue, NW., Washington, DC 20226.

Categories of individuals covered by the system:

(1) Criminal offenders or alleged criminal offenders acting alone or in concert with other individuals and suspects who have been or are under investigation for a violation or suspected violation of laws enforced by the Bureau; (2) Criminal offenders or alleged criminal offenders acting alone or in concert with individuals who have been referred to the Bureau of Alcohol, Tobacco, Firearms and Explosives by other law enforcement agencies, governmental entities, or the general public; (3) Informants; (4) Persons who come to the attention of the Bureau in the course of criminal investigations; (5) Persons who have been convicted of a crime punishable by imprisonment for a term exceeding one year and who have applied for relief from disability under Federal law with respect to the acquisition, receipt, transfer, shipment, or possession of firearms and explosives and whose disability was incurred by reason of such conviction; (6) Victims of crimes; (7) Witnesses.

Categories of records in the system:

(a) Records containing information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting of identifying data and notations of arrest, nature and disposition of criminal charges, sentencing, confinement, release, and parole/probation status; (b) Records containing information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; (c) Records containing reports identifiable to an individual compiling various stages of the process of enforcement of criminal laws from arrest or indictment to release from supervision; (d) Records compiled and maintained by the Bureau as generally described in (a), (b), and (c) above including the following: (1) Abandoned property reports; (2) ATF Criminal Investigation Reports; (3) ATF referrals to foreign, Federal, state, and local law enforcement agencies; (4) Chief and Regional Counsel opinions; (5) Contemporaneous investigative notes; (6) Criminal investigatory correspondence from and to foreign, Federal, state and local law enforcement agencies; (7) Criminal intelligence information on individuals suspected to be violating ATF laws and regulations; (8) Documentary proof of defendant's criminal record, identity, or lack of registration of National Firearms Act (N.F.A.) (as amended) firearm(s); (9) FBI Criminal Record Reports; (10) Fingerprints and palmprints; (11) Fugitive arrest warrants; (12) Handwriting exemplars; (13) Records of violations and reputation; (14) Illicit liquor and raw material surveys; (15) Laboratory reports of evidence analysis; (16) Memoranda of expected testimony of witnesses; (17) Organized crime members violating laws suspected of violating ATF laws; (18) Parole and pardon reports; (19) Personal histories (address, employment, social security number, financial background, physical description, etc.); (20) Photographs; (21) Purchase of evidence records; (22) Records of electronic surveillance by ATF; (23) Records received in response to summons and subpoenas; (24) Reliefs from disability; (25) Reports of interview with witnesses; (26) Search warrants and affidavits for search warrants; (27) Seized property reports; (28) Criminal records concerning firearms, explosives and alcohol; (29) Special agent's daily activity diary (accessible by agent only); (30) State and local law enforcement criminal investigative reports; (31) Statements of defendants; (32) Statements of witnesses; (33) Summons and subpoenas issued pursuant to criminal investigations; (34) Voice prints; (35) Wagering tax suspected violators; (36) Warrants and demand letters; (37) Criminal violation reports (a formal report compiling all or portions of the foregoing for prosecutive purposes).

Authority for maintenance of the system:

(1) 26 U.S.C. Chapter 40; (2) 26 U.S.C. Chapter 53, as amended; (3) 26 U.S.C. Chapters 54 through 80, as amended; (4) 18 U.S.C. Chapter 40; (5) 18 U.S.C. Chapter 44; (6) 18 U.S.C. Chapter 45.

Chapter 59; (7) 18 U.S.C. Chapter 114; (8) 22 U.S.C. 227; (9) 18 U.S.C. 1952; (10) Pub 107–296.

Purpose(s):

The purpose of this system is to suppress traffic in distilled spirits and tobacco products which taxes have not been paid; to enforce the Federal laws relating to the illegal possession and use of firearms, destructive devices, explosives, explosive materials; and to assist Federal, state, local and foreign law enforcement agencies in reducing crime and violence.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record in this system may be disclosed as a routine use:

A. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

B. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system's records.

C. To appropriate federal, state, local, foreign, or tribal law enforcement authorities for law enforcement purposes—criminal, civil, or regulatory.

D. To officials and employees of a federal agency or entity, including the White House, requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance of a security clearance; the execution of a security or suitability investigation; the classification of a job; or the issuance of a grant or benefit.

E. In an appropriate proceeding before a court or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding.

F. To an actual or potential party to litigation or the party's authorized representative for

purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

G. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

H. To federal, state, and local licensing agencies or associations, which require information concerning the suitability or eligibility of an individual for a license or permit.

I. To the General Services Administration and National Archives and Records Administration records management inspections conducted under the authority of 44 U.S.C. 2904 and

J. To a former employee of the Department for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

K. To such recipients and under such circumstances and procedures as are mandated by a federal statute or treaty.

L. To an organization or individual in either the public or private sector where there is reason to believe the recipient is or could become the target of a particular criminal activity or conspiracy to the extent the information is relevant to the protection of life or property.

M. To individuals and organizations in the course of an investigation to the extent necessary to obtain information pertinent to the investigation.

N. To Treasury Department, Alcohol and Tobacco Tax and Trade Bureau employees, when necessary to accomplish a Treasury Department or Department of Justice function relating to this system of records.

O. To criminal or national security intelligence gathering organizations for the purpose of identifying and suppressing the activities of international and national criminals and terrorism.

P. To insurance companies making determinations regarding claims in cases where the has conducted or is conducting an arson investigation.

Q. To unions recognized as exclusive bargaining representatives in accordance with prc contained in the Civil Service Reform Act of 1978, 5 U.S.C. 7111 and 7114.

R. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation case arising from the matters of which they complained and/or of which they were a vict

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Active records are stored in file folders in secure filing cabinets. Inactive records are stor file folders at Federal Records Centers. Records are also stored in electronic media.

Retrievability:

Records are retrieved by name, date of birth, social security number, other unique ident investigation number, serial number of firearm, or a combination of any of these; plus di geographical location of incident giving rise to investigation.

Safeguards:

Direct access restricted to personnel in the Department of Justice in the performance of duty. Transmitted to routine users on a need to know basis and to others upon verificati the substance and propriety of the request. Stored in lockable file cabinets in rooms loc during non-duty hours. The records stored in electronic media are password protected.

Retention and disposal:

Records are retained in accordance with General Records Schedules numbers 1 throug issued by the National Archives and Records Administration, and Bureau of Alcohol, To Firearms and Explosives Records Control Schedules numbers 101 and 201 and dispos

shredding or burning. Records on tape or on-line mass storage are disposed of by dega

System manager(s) and address:

Assistant Director, Firearms Explosive & Arson; Assistant Director, Field Operations; and Assistant Director, Science & Technology, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW, Washington, DC 20226.

Notification procedure:

See "Record access procedures" below.

Record access procedures:

For Records Accessible through the Privacy Act, mail a request in writing to the Disclosure Division, Privacy Act Request, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW., Washington, DC 20226, with the envelope and the letter marked "Privacy Access Request." The request should include a general description of records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. Some information may be exempt from access provisions as described in the section entitled "Exemptions claimed for the system." An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Record Access procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment, such as tax return information. Some information may be exempt from contesting record procedures described in the section entitled "Exemptions claimed for the system." An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

Record source categories:

Categories of individuals covered by the system: (1) Federal, state and local agencies; (2) witnesses; (3) employers; (4) professional organizations; (5) victims; (6) criminal offenders; (7) alleged criminal offenders; (8) fiscal records; (9) inspection records; (10) investigation records; (11) persons having knowledge of potential criminal activity; and (12) other persons listed in "Categories of individuals covered by the system" in this notice.

Exemptions claimed for the system:

Pursuant to 5 U.S.C. 552a(j)(2), the Attorney General has exempted records in this system from subsections (c)(3) and (4), (d)(1), (2), (3) and (4), (e)(1), (2) and (3), (e)(4)(G), (H), (e)(5) and (8), (f) and (g) of the Privacy Act. Rules have been promulgated in accordance with the requirement of 5 U.S.C. 553(b), (c) and (e) and are published in today's *Federal Register*.

[\[TOP\]](#)

JUSTICE/ATF.006

System name:

Internal Security Record System-Justice/ATF-006.

System location:

Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW
Washington, DC 20226.

Categories of individuals covered by the system:

(1) Present employees of the Bureau of ATF; (2) Former employees of the Bureau of ATF; (3) Applicants for employment; (4) Non-Bureau employees involved in criminal acts toward employees and Bureau property; (5) Individuals who were interviewed by Internal Affairs Special Agents; (6) Contract employees.

Categories of records in the system:

(1) Records containing investigative material compiled for law enforcement purposes including information relating to: (a) Conduct of employees and contract employees; (b) Integrity of employees; (2) Records containing investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or access to classified information including reports relating to security clearances of employees.

Authority for maintenance of the system:

18 U.S.C. 201, Executive Order 10450, Executive Order 11222.

Purpose(s):

This system is used to assure the Bureau Director, the Department of Justice, and the public that the Bureau is taking strong and vigorous steps to maintain the highest standards of integrity, loyalty, conduct, and security among Bureau personnel and contract employees. When a criminal investigation results in a compilation of information contained in this system, the information so compiled shall be transferred to the ATF Criminal Investigation Reporting System and shall become a part of that system for all purposes of the Privacy Act of 1974.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record in this system may be disclosed as a routine use:

A. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

B. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system's records.

C. In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, or

tribal law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.

D. To officials and employees of a federal agency or entity, including the White House, requiring information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance of a security clearance; the execution of a security or suitability investigation; the classification of a job; or the issuance of a grant or benefit.

E. In an appropriate proceeding before a court or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding.

F. To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

G. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

H. To federal, state, and local licensing agencies or associations, which require information concerning the suitability or eligibility of an individual for a license or permit.

I. To the General Services Administration and National Archives and Records Administration for records management inspections conducted under the authority of 44 U.S.C. 2904 and 2905.

J. To a former employee of the Department for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

K. To such recipients and under such circumstances and procedures as are mandated by a federal statute or treaty.

L. To an organization or individual in either the public or private sector where there is reasonable

believe the recipient is or could become the target of a particular criminal activity or conduct to the extent the information is relevant to the protection of life or property.

M. To individuals and organizations in the course of an investigation to the extent necessary to obtain information pertinent to the investigation.

N. To Treasury Department, Alcohol and Tobacco Tax and Trade Bureau employees, where necessary to accomplish a Treasury Department or Department of Justice function relating to this system of records.

O. To unions recognized as exclusive bargaining representatives in accordance with procedures contained in the Civil Service Reform Act of 1978, 5 U.S.C. 7111 and 7114.

P. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matter of which they complained and/or of which they were a victim.

Q. To designated officers and employees of state or local (including the District of Columbia) law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupy a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.

R. To the Office of Personnel Management, Merit Systems Protection Board, Equal Employment Opportunity Commission, Federal Labor Relations Authority, and the Office of Special Counsel for the purpose of properly administering Federal personnel systems and agencies' systems in accordance with applicable laws, Executive Orders, and regulations.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Active records stored in file folders in security filing cabinets and computer system (hard drive)
Inactive records stored in file folders at Federal Records Center.

Retrievability:

Records are retrieved by name.

Safeguards:

Direct access restricted to personnel in Department of the Justice in the performance of duty. Transmitted to routine users on a need to know basis and to others upon verification of the substance and propriety of the request. Stored in lockable metal file cabinets in room locked during non-duty hours.

Retention and disposal:

Records are retained in accordance with General Records Schedules Numbers 1 through 100 issued by the National Archives and Records Administration, and Bureau of Alcohol, Tobacco, Firearms and Explosives Records Control Schedules numbers 101 and 201 and disposed of by shredding or burning.

System manager(s) and address:

Assistant Director (Office of Inspection), Bureau of Alcohol, Tobacco, Firearms and Explosives
650 Massachusetts Avenue, NW, Washington, DC 20226.

Notification procedure:

See "Record access procedures" below.

Record access procedures:

For records accessible through the Privacy Act, address a request in writing to Disclosure Division, Privacy Act Request, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW., Washington, DC 20226, with the envelope and the letter clearly marked "Privacy Access Request." The request should include a general description of records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed, dated and either notarized or submitted under penalty of perjury. Some information may be exempt from access provisions as described in the section entitled "Exemptions claimed for the system." An individual who is the subject

record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Record Access procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment, such as tax return information. Some information may be exempt from contesting record procedures described in the section entitled "Exemptions claimed for the system." An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

Record source categories:

Examples include: (1) Employees of this Bureau; (2) Internal Investigative report forms; (3) Witnesses; (4) Informants; (5) Federal, state and local enforcement agencies; (6) Employers; (7) Educational institutions; (8) Credit agencies; (9) Neighbors; (10) References; (11) Professional Organizations; (12) Other government agencies; (13) Claimants; (14) Victims.

Exemptions claimed for the system:

Pursuant to 5 U.S.C. 552a(k)(5) (relating to security clearances) and (k)(2) (relating to confidentiality and integrity), the Attorney General has exempted records in this system from subsections (c)(3), (d)(1), (2), (3) and (4), (e)(1), (e)(4)(G), (H), and (I) and (f) of the Privacy Act. Rules have been promulgated in accordance with the requirement of 5 U.S.C. 553(b), (c) and (e) and are published in today's *Federal Register*.

[\[TOP\]](#)

JUSTICE/ATF-007

System name:

Personnel Record System-Justice/ATF-007.

System location:

Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW Washington, DC 20226. Components of this record system are geographically dispersed throughout the Bureau's field offices. A list of field offices is available by writing to the Civil Liberties Disclosure Division, Room 8400, 650 Massachusetts Avenue, NW, Washington, DC 202

Categories of individuals covered by the system:

(1) Present Employees of the Bureau of ATF; (2) Former Employees of the Bureau of ATF; (3) Applicants for employment with ATF.

Categories of records in the system:

Records include: (1) Allotment and Dues; (2) Annual Tax Reports; (3) Applicants for employment; (4) Applications for reassignment; (5) Awards, honors, and fellowship records; (6) Classification appeal records; (7) Death claim records; (8) Educational history; (9) Employment indebtedness records; (10) Employees qualified as Grievance Examiners; (11) Employee Suggestions; (12) Employee history; (13) Employee relations case file; (14) Equal employment opportunity records; (15) Health maintenance records; (16) Insurance records; (17) Military history; (18) Occupational injuries, disabilities, and Worker's Compensation Records; (19) Official personnel folder; (20) Outside employment and identification numbers, business and professional records; (21) Outside employment; (22) Outside financial interests; (23) Overtime and/or Premium Pay records; (24) Performance evaluation records; (25) Personal history; (26) Position description records; (27) Promotion/Selection Certificates Records; (28) Property custody records; (29) Retirement records; (30) Records of security clearance; (31) State career goals; (32) Supervisory or managerial potential records; (33) Temporary assignment and details; (34) Time application reports and records; (35) Training record; (36) U.S. Savings Bond participation records; (37) Upward mobility applications; (38) Vehicle accidents; (39) Withholding tax records; (40) Work schedule records; (41) Chief Counsel and Regional Counsel memoranda and opinions; (42) Government passport records.

Authority for maintenance of the system:

(1) 5 U.S.C. Chapter 29, Subchapter II; (2) 5 U.S.C. Chapters 31 and 33; (3) 5 U.S.C. C

43; (4) 5 U.S.C. Chapter 45; (5) 5 U.S.C. Chapter 51; (6) 5 U.S.C. Chapter 55, subchap (7) 5 U.S.C. Chapter 61; (8) 5 U.S.C. Chapter 75; (9) 5 U.S.C. Chapter 83; (10) 5 U.S.C. 31 CFR 2.28; 5 CFR 550.122, 550.183; (11) 5 U.S.C. 4503; (12) 5 U.S.C. 5101–5115; (13) 5 U.S.C. 7151–7154; (14) 5 U.S.C. 7901; (15) Public Law 92–261 (Equal Employment Act 1972); (16) Pub. L. 93–579; (Federal Employees Compensation Act); (17) Occupational and Health Act of 1970; (18) Executive Order 10561; (19) Executive Order 11222; (20) Executive Order 11478; (21) Executive Order 11491.

Purpose(s):

The purpose of this system is to provide a source of factual data about a person's Federal employment while in the service of the Bureau of Alcohol, Tobacco, Firearms and Explosives.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record in this system may be disclosed as a routine use:

A. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

B. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system's records.

C. In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, or tribal law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.

D. To officials and employees of a federal agency or entity, including the White House, who requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance of a security clearance; the execution of a security or suitability investigation; the classification of a job; or the issuance of a grant or benefit.

E. In an appropriate proceeding before a court or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding.

F. To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

G. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

H. To federal, state, and local licensing agencies or associations, which require information concerning the suitability or eligibility of an individual for a license or permit.

I. To the General Services Administration and National Archives and Records Administration records management inspections conducted under the authority of 44 U.S.C. 2904 and

J. To a former employee of the Department for purposes of: responding to an official inquiry of a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

K. To such recipients and under such circumstances and procedures as are mandated by a federal statute or treaty.

L. To an organization or individual in either the public or private sector where there is reason to believe the recipient is or could become the target of a particular criminal activity or conspiracy to the extent the information is relevant to the protection of life or property.

M. To individuals and organizations to the extent necessary to obtain relevant information needed by the Bureau to render a decision in regard to a personnel matter.

N. To Treasury Department, Alcohol and Tobacco Tax and Trade Bureau employees, with

necessary to accomplish a Treasury Department or Department of Justice function relating to this system of records.

O. To unions recognized as exclusive bargaining representatives in accordance with procedures contained in the Civil Service Reform Act of 1978, 5 U.S.C. 7111 and 7114.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Active records are stored in file folders in security filing cabinets. Inactive records are stored in file folders at Federal Records Centers. Records are also stored in electronic media.

Retrievability:

Records are retrieved by name, date of birth, social security number, employee identification number, or a combination of any of these four.

Safeguards:

Direct access is restricted to personnel in the Department of Justice in the performance of their duty. Records are transmitted to routine users on a need to know basis or where a right of access is established, and to others upon verification of the substance and propriety of request. These records are stored in lockable file cabinets in rooms locked during non-business hours. The records stored in electronic media are password protected.

Retention and disposal:

Records are retained in accordance with General Records Schedules numbers 1 through 5 issued by the National Archives and Records Administration, and Bureau of Alcohol, Tobacco, Firearms and Explosives Records Control Schedules numbers 101 and 201 and disposed of by shredding, burning or by degaussing.

System manager(s) and address:

Assistant Director, Office of Science and Technology; Assistant Director, Public and

Governmental Affairs; and Assistant Director, Management/Chief Financial Officer, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW, Washington, DC 20226.

Notification procedure:

See "Record access procedures" below.

Record access procedures:

For records accessible through the Privacy Act, mail a request in writing to the Disclosure Division, Privacy Act Request, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW, Washington, DC 20226, with the envelope and the letter clearly marked "Privacy Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed, dated, and either notarized or submitted under penalty of perjury. Some information may be exempt from access provisions as described in the section entitled "Exemptions claimed for the system." An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Record Access procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment, such as tax return information. Some information may be exempt from contesting record procedures described in the section entitled "Exemptions claimed for the system." An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

Record source categories:

Examples include: (1) Administrative Records; (2) Applicants for employment with the B

(3) Acquaintances; (4) Business and professional associates; (5) Creditors; (6) Criminal records; (7) Educational Institutions attended; (8) Employee records; (9) Equal Employment Opportunity Commission; (10) Financial institutions; (11) Fiscal records; (12) Former employees; (13) Former employers; (14) Inspection records; (15) Internal investigation records; (16) Internal Revenue Service; (17) Military records; (18) Outside employers; (19) Physicians; (20) Police reports; (21) Position classification specialists; (22) Psychiatrists; (23) Referees; (24) Supervisors; (25) Training officers; (26) Unions, accredited; (27) Office of Personnel Management; (28) Witnesses.

Exemptions claimed for the system:

Pursuant to 5 U.S.C. 552a(k)(5) the Attorney General has exempted records in this system from subsections (c)(3), (d)(1), (2), (3) and (4), (e)(1), (e)(4)(G), (H), and (I) and (f) of the Privacy Act. Rules have been promulgated in accordance with the requirement of 5 U.S.C. 553(b), (c) and (e) and are published in today's *Federal Register*.

[\[TOP\]](#)

JUSTICE/ATF-008

System name:

Regulatory Enforcement Record System—Justice/ATF-008.

System location:

Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW Washington, DC 20226. Components of this system of records are also geographically dispersed throughout ATF's district and field offices. A list of field offices is available by request to the Chief, Disclosure Division, Room 8400, 650 Massachusetts Avenue, NW, Washington, DC 20226.

Categories of individuals covered by the system:

Individuals who have been issued permits or licenses, have filed applications with ATF, registered with ATF, or are responsible persons or employees of a licensee or permittee to the extent that the records concern private individuals or entrepreneurs, including, but not limited to:

to: (a) Explosives licensees, employees and responsible persons; (b) Claimants for refund taxes; (c) Federal Firearms Licenses, employees and responsible persons (d) Collectors of firearms or ammunition; (e) Importers of firearms or ammunition, and (f) Users of explosives materials.

Categories of records in the system:

Records containing investigative material compiled for law enforcement purposes which consist of the following: (1) Abstracts of offers in compromise; (2) Administrative law judgments; (3) Assessment records: (a) notices of proposed assessments, (b) notices of shortages or losses, (c) notices to IRS to assess taxes, (d) recommendation for assessment; (4) Claim records: (a) claims; (b) letters of claim rejection; (c) sample reports; (d) supporting data; (e) vouchers and schedules of payment; (5) Comments on proposed rulemakings; (6) Complaints from third parties; (7) Correspondence concerning records in this system and related matters; (8) Financial statements; (9) Inspection and investigation reports; (10) Judgments and demands on principals and sureties for payment of excise tax liabilities; (11) Letters of reprimand; (12) Lists of permittees and licensees; (13) Lists of officers, directors and principal stockholders; (14) Mailing lists and addressograph plates; (15) Notices of delinquent registration; (16) Offers in compromise; (17) Operation records: (a) Operating reports, (b) reports of required inventories, (c) reports of thefts or losses of firearms, (d) reports of thefts of explosives materials, (e) transaction records, (f) transaction reports; (18) Orders of revocation, suspension or annulment of permits or licenses; (19) District and Chief Counsel opinions and memoranda; (20) Reports of violations; (21) Permit status records; (22) Qualifying and background records: (a) access authorizations, (b) advertisement records, (c) applications, (d) bonds, (e) business histories, (f) criminal records, (g) diagrams of premises, (h) educational histories, (i) employment histories, (j) environmental records, (k) financial data, (l) formula approvals, (m) label approvals, (n) licenses, (o) notices, (p) permits, (q) personal references, (r) plant permits, (s) plant capacities, (t) plats and plans, (u) registrations, (v) sample reports, (w) signature authorities, (x) special permissions and authorizations, (y) statements of process; (23) Suspension orders; (24) Tax records: (a) control cards relating to periodic payment and preparation of taxes, (b) excise and special tax returns, (c) notices of tax discrepancy or adjustment.

Authority for maintenance of the system:

(1) 26 U.S.C. 7011; (2) 18 U.S.C. 923(a); (3) 18 U.S.C. 923(b); (4) 18 U.S.C. 843(a); (5) 18 U.S.C. 2278; (6) 26 U.S.C. 6001; (7) 26 U.S.C. 6011(a); (8) 26 U.S.C. 6201; (9) 26 U.S.C. 6202; (10) 18 U.S.C. 843(d); (11) 18 U.S.C. 923(f); (12) Pub. L. 107-296.

Purpose(s):

The purpose of this system is to determine suitability, eligibility or qualifications of individuals who are engaged or propose to engage in activities regulated by ATF; achieve compliance with laws under ATF's jurisdiction; interact with Federal, state and local governmental agencies; assist in the resolution of problems relating to industrial development, revenue protection, public safety, ecology, and other areas of joint jurisdictional concern. When a criminal investigation requires a compilation of information contained in this system of records, the information shall be transferred to the Justice/ATF—Criminal Investigation Report System and shall become a part of that system for all purposes of the Privacy Act of 1974.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record in this system may be disclosed as a routine use:

- A. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
- B. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system's records.
- C. In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, or tribal law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.
- D. To officials and employees of a federal agency or entity, including the White House, who requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance of a security clearance; the execution of a security or suitability investigation; the classification of a job; or the issuance of a grant or benefit.

E. In an appropriate proceeding before a court or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding.

F. To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

G. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

H. To federal, state, and local licensing agencies or associations, which require information concerning the suitability or eligibility of an individual for a license or permit.

I. To the General Services Administration and National Archives and Records Administration records management inspections conducted under the authority of 44 U.S.C. 2904 and

J. To a former employee of the Department for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

K. To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

L. To an organization or individual in either the public or private sector where there is reason to believe the recipient is or could become the target of a particular criminal activity or conspiracy to the extent the information is relevant to the protection of life or property.

M. To individuals and organizations to the extent necessary to obtain or verify information pertinent to the Bureau's decision to grant, deny or revoke a license or permit, or pertaining to an ongoing investigation.

N. To Treasury Department, Alcohol and Tobacco Tax and Trade Bureau employees, where necessary to accomplish a Treasury Department or Department of Justice function relating to this system of records.

O. To national and international intelligence gathering organizations for the purpose of identifying international and national criminals involved in consumer fraud, revenue evasion, and other crimes.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records are stored in file folders in filing cabinets and in electronic media.

Retrievability:

Records are retrieved by name, permit or license number, by document locator number, by employer identification number (EIN).

Safeguards:

Direct access restricted to personnel in the Department of Justice in the performance of their duty. Transmitted to routine users on a need to know basis and others upon verification of the substance and propriety of the request. Stored in file cabinets in rooms locked during non-business hours. The records stored in electronic media are password protected.

Retention and disposal:

Records are retained in accordance with General Records Schedules numbers 1 through 5 issued by the National Archives and Records Administration, and Bureau of Alcohol, Tobacco, Firearms and Explosives Records Control Schedules numbers 101 and 201 and disposed of by shredding, burning or by degaussing.

System manager(s) and address:

Assistant Director, Firearms Explosive & Arson; Field Operations; and Assistant Director

Science & Technology, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650
Massachusetts Avenue, NW, Washington, DC 20226.

Notification procedure:

See "Record access procedures" below.

Record access procedures:

For Records Accessible through the Privacy Act, mail a written request to the Disclosure Division, Privacy Act Request, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW, Washington, DC 20226, with the envelope and the letter card marked "Privacy Access Request." The request should include a general description of records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed, dated, and either notarized or submitted under penalty of perjury. Some information may be exempt from access provisions as described in the section entitled "Exemptions claimed for the system." An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Record Access procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment, such as tax return information. Some information may be exempt from contesting record procedures described in the section entitled "Exemptions claimed for the system." An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

Record source categories:

Examples include: (1) Acquaintances; (2) Bureau personnel; (3) Business and professional associates; (4) Creditors; (5) Criminal records; (6) Financial institutions; (7) Former employees

(8) Internal Revenue Service; (9) Military records; (10) Physicians; (11) Psychiatrists; (12) References; (13) Police reports; (14) Witnesses; (15) Federal law enforcement agencies; (16) State law enforcement agencies; (17) Local law enforcement agencies; (18) State regulatory agencies; (19) Federal regulatory agencies; (20) Local regulatory agencies; (21) Chief Counsel's opinions; (22) Regional Counsel's opinions; (23) Chief Counsel's memoranda; (24) Regional Counsel's memoranda; (25) Field investigation reports; (26) Third parties.

Exemptions claimed for the system:

Pursuant to 5 U.S.C. 552a(k)(2), the Attorney General has exempted records in this system from subsections (c)(3), (d)(1), (2), (3) and (4), (e)(1), (e)(4)(G), (H), and (I) and (f) of the Privacy Act. Rules have been promulgated in accordance with the requirement of 5 U.S.C. 553(b), (c) and (e) and are published in today's *Federal Register*.

[\[TOP\]](#)

JUSTICE/ATF-009

System name:

Technical and Scientific Services Record System Justice/ATF-009.

System location:

Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW Washington, DC 20226. Components of this record system are geographically dispersed throughout Bureau of Alcohol, Tobacco, Firearms and Explosives' field offices. A list of field offices is available by writing to the Chief, Disclosure Division, Room 8400, 650 Massachusetts Avenue, NW, Washington, DC 20226.

Categories of individuals covered by the system:

Individuals covered may include: (1) Applicants to register firearms under the National Firearms Act; (2) Importers of implements of war as defined under the Mutual Security Act of 1954 and the Arms Export Control Act of 1976; (3) Licensed importers registered under the Mutual Security Act of 1954 and the Arms Export Control Act of 1976; (4) Manufacturers of National Firearms Act firearms that are exempt from payment of Special (Occupational) tax provided

(5) Non-Bureau chemists certified to make analysis of alcoholic beverages; (6) Persons involved in explosives tagging and detection program; (7) Registered owners of National Firearms Act firearms; (8) Special (Occupational) taxpayers as defined under Title II of the Internal Revenue Control Act of 1968; (9) Victims of explosives; (10) Individuals involved in Government funded research projects.

Categories of records in the system:

Records may include: (1) Alteration records of registered National Firearms Act firearms; (2) Applications to register firearms and destructive devices under the National Firearms Act; (3) Applications to import articles on the United States Munitions list; (4) Blueprints; (5) Certifications of payment of Special (occupational) tax payments; (6) Changes of address of owner of firearms registered under the National Firearms Act; (7) Claims for erroneous Special (Occupational) taxes payments; (8) Descriptions of Inventions; (9) Delinquency notices regarding proof of importation of National Firearms Act firearms; (10) Explosive reports; (11) Non-Bureau chemists' statements of qualification; (12) Patent information; (13) Registrations of firearms and destructive devices under the National Firearms Act; (14) Registration of trophy firearms; (15) Requests and authorizations for temporary movement and/or temporary storage of National Firearms Act firearms; (16) Technical and scientific data; (17) Transfer records concerning National Firearms Act firearms; (18) Trade secrets; (19) United States Government contracts to manufacturers of National Firearms Act firearms; (20) Chief Counsel and Regional Counsel memoranda and opinions.

Authority for maintenance of the system:

(1) 18 U.S.C. Chapter 40; (2) 18 U.S.C. Chapter 44; (3) 26 U.S.C. 6001(a); (4) 26 U.S.C. 6011; (5) 26 U.S.C. 7011; (6) Executive Order 11958; (7) Pub. L. 107-296.

Purpose(s):

The purpose of this system is to provide technical, investigative and scientific support and expertise to Criminal and Regulatory Enforcement activities of the Bureau; to other Federal, state, local and foreign law enforcement agencies; and to provide scientific support and expertise to those industries involved in activities regulated by the Bureau. When a criminal investigation results in a compilation of information contained in this system, the information compiled shall be transferred to the Justice/ATF—Criminal Investigation Report System and shall become a part of that system for all purposes of the Privacy Act of 1974.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record in this system may be disclosed as a routine use:

A. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

B. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system's records.

C. In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, or tribal law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.

D. To officials and employees of a federal agency or entity, including the White House, who requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance of a security clearance; the execution of a security or suitability investigation; the classification of a job; or the issuance of a grant or benefit.

E. In an appropriate proceeding before a court or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding.

F. To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

G. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

H. To federal, state, and local licensing agencies or associations, which require information concerning the suitability or eligibility of an individual for a license or permit.

I. To the General Services Administration and National Archives and Records Administration records management inspections conducted under the authority of 44 U.S.C. 2904 and

J. To a former employee of the Department for purposes of: responding to an official inquiry of a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

K. To such recipients and under such circumstances and procedures as are mandated by a federal statute or treaty.

L. To an organization or individual in either the public or private sector where there is reason to believe the recipient is or could become the target of a particular criminal activity or conduct, to the extent the information is relevant to the protection of life or property.

M. To individuals and organizations to the extent necessary to obtain or verify information pertinent to the Bureau's decision to grant, deny, or revoke a license or permit, or pertinent to an ongoing investigation.

N. To Treasury Department, Alcohol and Tobacco Tax and Trade Bureau employees, where necessary to accomplish a Treasury Department or Department of Justice function relating to this system of records.

O. To insurance companies making determinations regarding claims in cases where the Bureau has conducted or is conducting an arson investigation.

P. To national and international intelligence gathering organizations for the purpose of identifying international and national criminals involved in consumer fraud, revenue evasion, and other crimes.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of

in the system:***Storage:***

Records are stored in file folders and in electronic media.

Retrievability:

Records are retrieved by name, by other unique identifier, control number, serial number, National Firearms Act firearms.

Safeguards:

Records are stored in file cabinets locked during non-duty hours. The records stored in electronic media are password protected.

Retention and disposal:

Records are retained in accordance with General Records Schedules numbers 1 through 100 issued by the National Archives and Records Administration, and Bureau of Alcohol, Tobacco, Firearms and Explosives Records Control Schedules numbers 101 and 201 and disposed of by shredding or burning. Records stored on tape discs or on-line mass storage are disposed of by degaussing.

System manager(s) and address:

Assistant Director, Firearms Explosive & Arson; Assistant Director, Field Operations; and Assistant Director, Science & Technology, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW, Washington, DC 20226.

Notification procedure:

See "Record access procedures" below.

Record access procedures:

If records are accessible through the Privacy Act, mail a written request to the Disclosure Division, Privacy Act Request, Bureau of Alcohol, Tobacco, Firearms and Explosives, 65

Massachusetts Avenue, NW, Washington, DC 20226, with the envelope and the letter c marked "Privacy Access Request." The request should include a general description of records sought and must include the requester's full name, current address, and date a place of birth. The request must be signed, dated, and either notarized or submitted un penalty of perjury. Some information may be exempt from access provisions as describe the section entitled "Exemptions claimed for the system." An individual who is the subje record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should di their request according to the Record Access procedures listed above, stating clearly ar concisely what information is being contested, the reasons for contesting it, and the pro amendment to the information sought. Some information is not subject to amendment, : tax return information. Some information may be exempt from contesting record procedi described in the section entitled "Exemptions claimed for the system." An individual who subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

Record source categories:

Examples include: (1) Individuals; (2) Companies; (3) Corporations; (4) Firearms License Explosive Licensees; (6) Explosive Permittees; (7) Bureau personnel; (8) Federal law enforcement agencies; (9) State law enforcement agencies; (10) Local law enforcement agencies; (11) Foreign law enforcement agencies; (12) Federal Regulatory agencies; (1 Regulatory agencies; (14) Local Regulatory agencies; (15) Non-Bureau Chemists.

Exemptions claimed for the system:

Pursuant to 5 U.S.C. 552a(k)(2), the Attorney General has exempted records in this sys from subsections (c)(3), (d)(1), (2),(3) and (4), (e)(1), (e)(4)(G), (H), and (I) and (f) of the Privacy Act. Rules have been promulgated in accordance with the requirement of 5 U.S 553(b), (c) and (e) and are published in today's *Federal Register*.

[\[TOP\]](#)

JUSTICE/ATF-010

System name:

Training and Professional Development Record System-Treasury/ATF-010.

System location:

Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW Washington, DC 20226. Components of this record system are geographically disperse throughout the Bureau's field offices. A list of field offices is available by writing to the C Disclosure Division, 650 Massachusetts Avenue, NW, Washington, DC 20226.

Categories of individuals covered in the system:

Non-ATF individuals applying for ATF training and/or professional development; those instructors for ATF training and/or professional development; possible emergency contact and/or supervisors' names are collected from the trainee.

Categories of records in the system:

Records may include: (a) Name, (b) office address, (c) telephone number, (d) fax number, (e) social security information, (f) firearms qualifications, (g) eligibility of instructors, (h) certifications held by instructors, (i) courses previously taught by instructors, (j) home address, (k) date of birth, (l) position title, (m) length of time in public service, (n) time on current assignment, (o) number of years in current position, (p) name and telephone number of immediate supervisor, (q) education experience, (r) related occupational experience, (s) blood type, (t) military experience, (u) law enforcement experience, (v) description of duties and responsibilities, (w) internet address, (x) pager number, (y) smoking preference, (z) Chief Counsel and Regional Counsel memoranda and opinions, and (aa) other information as required for training or instructor determination or safety.

Authority for maintenance of the system:

5 U.S.C. 4104; Executive Order No. 11348 as amended by Executive Order No. 12107 (

Purpose(s):

The purpose of this system is to provide basic data about ATF instructors and those trained by ATF.

Routine uses of records maintained in the system, including categories of users, and purposes of such uses:

A record in this system may be disclosed as a routine use:

- A. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
- B. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system's records.
- C. In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, or tribal law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.
- D. To officials and employees of a federal agency or entity, including the White House, when such officials or employees require information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance of a security clearance; the execution of a security or suitability investigation; the classification of a job; or the issuance of a grant or benefit.
- E. In an appropriate proceeding before a court or administrative or regulatory body when records are determined by the Department of Justice to be arguably relevant to the proceeding.
- F. To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion on such matters as settlement, plea bargaining, or

informal discovery proceedings.

G. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

H. To federal, state, and local licensing agencies or associations, which require information concerning the suitability or eligibility of an individual for a license or permit.

I. To the General Services Administration and National Archives and Records Administration records management inspections conducted under the authority of 44 U.S.C. 2904 and

J. To a former employee of the Department for purposes of: responding to an official inquiry from a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

K. To such recipients and under such circumstances and procedures as are mandated by a federal statute or treaty.

L. To an organization or individual in either the public or private sector where there is reason to believe the recipient is or could become the target of a particular criminal activity or conspiracy to the extent the information is relevant to the protection of life or property.

M. To individuals and organizations to the extent necessary to verify their qualifications and eligibility for training.

N. To Treasury Department, Alcohol and Tobacco Tax and Trade Bureau employees, where necessary to accomplish a Treasury Department or Department of Justice function relating to this system of records.

O. To unions recognized as exclusive bargaining representatives in accordance with procedures contained in the Civil Service Reform Act of 1978, 5 U.S.C. 7111 and 7114.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Paper records are stored in security filing cabinets. Records are also stored in electronic media.

Retrievability:

Records are retrieved by name, agency and/or office location, social security number or the above.

Safeguards:

Paper records are kept in locked filing cabinets in locked rooms during non-business hours. Electronic media records are password protected.

Retention and disposal:

Records are retained in accordance with General Records Schedules numbers 1 through 100 issued by the National Archives and Records Administration, and the Bureau of Alcohol Tobacco, Firearms and Explosives Control Schedules number 101 and 201 and disposed of by shredding, burning or by degaussing.

System manager(s) and address:

Assistant Director, Training and Professional Development, Bureau of Alcohol, Tobacco, Firearms and Explosives, 650 Massachusetts Avenue, NW, Washington, DC 20226.

Notification procedure:

See "Record access procedures" below.

Record access procedures:

For records accessible through the Privacy Act, mail a request in writing to the Disclosure Officer.

Division, Privacy Act Request, Bureau of Alcohol, Tobacco, Firearms and Explosives, 65 Massachusetts Avenue, NW, Washington, DC 20226, with the envelope and the letter c marked "Privacy Access Request." The request should include a general description of records sought and must include the requester's full name, current address, and date & place of birth. The request must be signed and dated and either notarized or submitted penalty of perjury.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Record Access procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment, including tax return information.

Record source categories:

Examples include: Administrative records, applications submitted by non-ATF individual seeking ATF training and applications submitted by instructors.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

Antitrust Division

JUSTICE/ATR-001

System name:

Antitrust Division Expert Witness File.

System location:

U.S. Department of Justice, 10th & Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

Individuals who have served in the capacity of an expert for the Department of Justice in connection with civil or criminal antitrust litigation.

Categories of records in the system:

This system contains the names of persons used by the Antitrust Division in an expert capacity and also indicates the area of their specialty, the type of service rendered, the fees paid, and the dates on or during which such services were performed.

Authority for maintenance of the system:

Authority for the establishment and maintenance of this system exists under 44 U.S.C. 3501 and 28 U.S.C. 522.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

This system is routinely used by trial attorneys of the Antitrust Division when considering selection of experts as witnesses for the development or presentation of specific antitrust cases. The system also serves as a reference resource for Division personnel in compiling statistical information or reports regarding the actual or anticipated costs of litigation.

A record maintained in this system, or any facts derived therefrom, may be disseminated in a proceeding before a court or adjudicative body before which the Antitrust Division is authorized to appear, when (1) the Antitrust Division, or any subdivision thereof; or (2) any employee of the Antitrust Division in his or her official capacity; or (3) any employee of the Antitrust Division in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (4) the United States, or any agency or subdivision thereof; or (5) the United States, where the Antitrust Division determines that the litigation is likely to affect it or any subdivision, is a party to litigation or has an interest in litigation and such records are determined by the Antitrust Division to be arguably relevant to the litigation.

Release of information to the news media:

Information permitted to be released to the news medias and the public pursuant to 28

50.2 may be made available from systems of records maintained by the Department of Justice, unless it is determined that release of the specific information in the context of a particular request would constitute an unwarranted invasion of personal privacy.

Release of information to members of Congress:

Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on the individual who is the subject of the record.

Release of information to the National Archives and Records Administration:

A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in this system is contained in documents organized in individual folders.

Retrievability:

Information is retrieved primarily by using the name of the individual called as an expert witness for the Government in antitrust cases brought by the Department.

Safeguards:

Information contained in the system is unclassified. During working hours access to the is controlled and monitored by Antitrust Division personnel in the area where the system maintained; during non-duty hours all doors to that area are locked.

Retention and disposal:

Indefinite.

System manager(s) and address:

Executive Officer, Antitrust Division, U.S. Department of Justice, 10th & Constitution Ave NW, Washington, DC 20530.

Notification procedure:

Address inquiries to the Assistant Attorney General, Antitrust Division, U.S. Department Justice, 10th & Constitution Avenue NW, Washington, DC 20530.

Record access procedures:

Requests for access to a record from this system shall be in writing and be clearly identify a "Privacy Access Request" . Including in the request should be the name of the person presented as an expert witness for the Government and the name of the case in which services were rendered. The requester should indicate a return address. Requests will be directed to the System Manager shown above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their requests to the System Manager and state clearly and concisely when information being contested, the reasons for contesting it and the proposed amendment to the information sought.

Record source categories:

Sources of information maintained in this system are those records reflecting the communication between the individual and the Department of Justice (including matters of compensation and staff attorneys or other employees directly involved with the individual in the preparation and conduct of the litigation).

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/ATR-003

System name:

Index of Defendants in Pending and Terminated Antitrust Cases.

System location:

U.S. Department of Justice: Liberty Place, Suite 200, Washington, DC 20530.

Categories of individuals covered by the system:

Individual defendants in pending and terminated criminal and civil cases brought by the States under the antitrust laws.

This system contains an index reference to the case in which an individual (or corporation) was a defendant; included information is proper case name, the judicial district and number of the case, and the date filed.

Authority for maintenance of the system:

Authority for the establishment and maintenance of this index system exists under 28 U.S.C. 522 and 44 U.S.C. 3101.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Routine use of this cross index system is generally made by Department personnel for reference to proper case name. In addition a compilation of antitrust cases filed is prepared showing the names of all defendants in pending civil and criminal Government antitrust cases. This compilation is utilized within the Department and occasionally distributed to other Government agencies for reference and statistical purposes.

A record maintained in this system, or any facts derived therefrom, may be disseminated in a proceeding before a court or adjudicative body before which the Antitrust Division is authorized to appear, when (1) the Antitrust Division, or any subdivision thereof; or (2) any employee of the Antitrust Division in his or her official capacity; or (3) any employee of the Antitrust Division in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (4) the United States, or any agency or subdivision thereof; or (5) the United States, where the Antitrust Division determines that the litigation is likely to affect it or any of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the Antitrust Division to be arguably relevant to the litigation.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Information in the system is maintained on index cards.

Retrievability:

Information in the system is retrieved by reference to the name of individual or corporate defendants in antitrust cases.

Safeguards:

Information contained in the system is unclassified and of a public nature. During work hours access to the index is monitored by Antitrust Division personnel; during non-duty the area in which the system is maintained is locked.

Retention and disposal:

Indefinite.

System manager(s) and address:

Chief, Freedom of Information Act/Privacy Act Unit, Antitrust Division, U.S. Department of Justice, Liberty Place, Suite 200, Washington, DC 20530.

Notification procedure:

Address inquiries to the Assistant Attorney General, Antitrust Division, U.S. Department of Justice, Washington, DC 20530.

Record access procedures:

Requests for access to a record from this system shall be in writing and be clearly identified as a "Privacy Access Request". Included in the request should be the name of the defendant pending or terminated Government antitrust litigation. Requesters should indicate a return

address. Requests will be directed to the System Manager shown above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the index should direct request to the System Manager and state clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in this index are complaints filed under the antitrust laws of the United States and from Department records relating to such cases.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/ATR-004

System name:

Statements by Antitrust Division Officials (ATD Speech File).

System location:

U.S. Department of Justice, Liberty Place, Suite 200, Washington, DC 20530.

Categories of individuals covered by the system:

Past and present employees of the Antitrust Division.

Categories of records in the system:

This system contains an index record for each public statement or speech issued or made

employees of the Antitrust Division.

Authority for maintenance of the system:

Authority for maintaining this system exists under 44 U.S.C. 3101.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

This index is maintained for ready reference by Department personnel for the identification of the subject matter of and persons originating public statements by Antitrust Division employees; such reference is utilized in aid of compliance with requests from the public within the agency for access to texts of such statements.

A record maintained in this system, or any facts derived therefrom, may be disseminated in a proceeding before a court or adjudicative body before which the Antitrust Division is authorized to appear, when (1) the Antitrust Division, or any subdivision thereof; or (2) any employee of the Antitrust Division in his or her official capacity; or (3) any employee of the Antitrust Division in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (4) the United States, or any agency or subdivision thereof; or (5) the United States, where the Antitrust Division determines that the litigation is likely to affect it or any of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the Antitrust Division to be arguably relevant to the litigation.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 44 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose

relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information contained in the index system is maintained on index cards.

Retrievability:

This reference index utilizes name of present and former employees making or issuing statements as well as the subject matter or title of the statement.

Safeguards:

Information contained in the system is unclassified. During duty hours personnel monitor access to this index; the area is locked during non-duty hours.

Retention and disposal:

Indefinite.

System manager(s) and address:

Chief, Freedom of Information Act/Privacy Act Unit, Antitrust Division, U.S. Department of Justice, Liberty Place, Suite 200, Washington, DC 20530.

Notification procedure:

Address inquiries to the Assistant Attorney General, Antitrust Division, U.S. Department of Justice, 10th and Constitution Avenue NW, Washington, DC 20530.

Record access procedures:

Request for access to a record from this system should be made in writing and be clearly identified as a "Privacy Access Request". Included in the request should be the name of the Antitrust Division employee making or issuing a public statement. Requesting party should include a return address. Requests will be directed to the System Manager shown above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the index should direct request to the System Manager and state clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information maintained in the index are those records reflecting public statements issued or made by Antitrust Division employees.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/ATR-005

System name:

Antitrust Information Management System (AMIS)—Time Reporter.

System location:

U.S. Department of Justice, 10th and Constitution Ave., NW, Washington, DC 20530.

Categories of individuals covered by the system:

Professional employees of the Antitrust Division of the U.S. Department of Justice.

Categories of records in the system:

The file contains the employees' name and allocations of his/her work time.

Authority for maintenance of the system:

The file will be established and maintained pursuant to the following authorities: 28 C.F.R. 0.40(f), 28 U.S.C. 522, 31 U.S.C. 11, 31 U.S.C. 66a, 5 U.S.C. 301, and 2 U.S.C. 601.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The file is used by Antitrust Division personnel to keep track of resources and as a basis for determining Antitrust Division allocations of resources (professional time) to particular products and industries (e.g., oil, auto, chemicals) and to broad categories of resource use such as conspiratorial conduct, oligopoly and monopoly, civil cases, criminal cases, and proceedings before regulatory agencies. In addition, the file will be employed in the preparation of reports for the Division's budget requests and to the Attorney General and Congress.

A record maintained in this system, or any facts derived therefrom, may be disseminated in a proceeding before a court or adjudicative body before which the Antitrust Division is authorized to appear, when (1) the Antitrust Division, or any subdivision thereof; or (2) any employee of the Antitrust Division in his or her official capacity; or (3) any employee of the Antitrust Division in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (4) the United States, or any agency or subdivision thereof; or (5) the United States, where the Antitrust Division determines that the litigation is likely to affect it or any of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the Antitrust Division to be arguably relevant to the litigation.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from the system of records may be disclosed to NARA and GSA for records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are maintained electronically in the AMIS computerized information system.

Retrievability:

Information is retrieved by a variety of key words, including names of individuals.

Safeguards:

Information contained in the system is unclassified. It is safeguarded and protected in accordance with Department rules and procedures governing the handling of computer information. Access to the file is limited to those employees whose official duties require access.

Retention and disposal:

Information contained in the file is retained indefinitely.

System manager(s) and address:

Chief, Information Systems Support Group, Antitrust Division, U.S. Department of Justice
4th Street NW, Room 11-854, Washington, DC 20001.

Notification procedure:

Same as System Manager.

Record access procedures:

Same as Notification.

Contesting record procedures:

Same as Notification.

Record source categories:

Information on time allocation is provided by Antitrust Division section and field office ch

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/ATR-006

System name:

Antitrust Information Management System (AMIS)-Matter Report.

System location:

U.S. Department of Justice, 10th and Constitution Avenue, NW., Washington, DC 20530

Categories of individuals covered by the system:

Professional employees of the Antitrust Division of the U.S. Department of Justice and individual defendants and investigation targets involved in past and present Antitrust investigations and cases.

Categories of records in the system:

The system contains the names of Division employees and their case/investigation assignments and the names of individual defendants/investigation targets as they relate to specific case/investigation. In addition, information reflecting the current status and handling of Antitrust cases/investigations is included within this system.

Authority for maintenance of the system:

The file is established and maintained pursuant to 28 CFR 40(f), 28 U.S.C. 522, and 44 U.S.C. 3101.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The file is used by Antitrust Division personnel as a basis for determining Antitrust Division allocation of resources to particular products and industries (e.g., oil, autos, chemicals), broad categories of resource use such as civil cases, criminal cases, regulatory agency and Freedom of Information Act requests. It is employed by the section chiefs, the Deputy Director of Operations, and other Division personnel to ascertain the progress and current status of cases and investigations within the Division. In addition, the files will be employed in the preparation of reports for the Division's budget requests and to the Attorney General and Congress.

A record maintained in this system, or any facts derived therefrom, may be disseminated

1. In a proceeding before a court or adjudicative body before which the Antitrust Division is authorized to appear, when (1) the Antitrust Division, or any subdivision thereof; or (2) an employee of the Antitrust Division in his or her official capacity; or (3) any employee of the Antitrust Division in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (4) the United States, where the Antitrust Division determines the litigation is likely to affect it or any of its subdivisions, is a party to litigation or has an

interest in litigation and such records are determined by the Antitrust Division to be argu relevant to the litigation.

2. In any health care-related civil or criminal case, investigation, or matter, information indicating patient harm, neglect, or abuse, or poor or inadequate quality of care, at a health care facility or by a health care provider, may be disclosed as a routine use to any federal, state, local, tribal, foreign, joint, international or private entity that is responsible for regulating, licensing, registering, or accrediting any health care provider or health care facility, or enforcing any health care-related laws or regulations. Further, information indicating an ongoing quality of care problem by a health care provider or at a health care facility may be disclosed to an appropriate health plan. Additionally, unless otherwise prohibited by applicable law, information indicating patient harm, neglect, abuse, or poor or inadequate quality of care may be disclosed to the affected patient or his or her representative or guardian at the discretion and in the manner determined by the agency in possession of the information.

3. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

4. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record. Information not otherwise required to be released pursuant to 5 U.S.C. 552 may be made available.

5. To the National Archives and Records Administration and to the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Information relating to health care fraud may be disclosed to private health plans, or

associations of private health plans, and health insurers, or associations of health insurers, for the following purposes: to promote the coordination of efforts to prevent, detect, investigate, and prosecute health care fraud; to assist efforts by victims of health care fraud to obtain restitution; to enable private health plans to participate in local, regional, and national health care fraud task force activities; and to assist tribunals having jurisdiction over claims against private health plans.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are maintained electronically in the Information systems support group's AMIS Computerized information system.

Retrievability:

Information is retrieved by a variety of key words.

Safeguards:

Information contained in the system is unclassified. It is safeguarded and protected in accordance with Department rules and procedures governing the handling of computer information. Access to the file is limited to those persons whose official duties require such access and employees of the Antitrust Division.

Retention and disposal:

Information contained in the file is retained indefinitely.

System manager(s) and address:

Chief, Information Systems Support Group; Antitrust Division; U.S. Department of Justice
4th Street, NW., Room 11-854, Washington, DC 20001.

Notification procedure:

Address inquiries to the Assistant Attorney General, Antitrust Division, U.S. Department

Justice, 10th and Constitution Avenue, Washington, DC. 20530.

Record source categories:

Information for the monthly report is provided by the Antitrust Division section and filed with the chiefs.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3), (d), (e)(4)(G)– and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/ATR–007

System name:

Antitrust Division Case Cards.

System location:

U.S. Department of Justice, Liberty Place, Suite 200, Washington, DC 20530.

Categories of individuals covered by the system:

Individual defendants in pending and terminated criminal and civil cases brought by the States under the antitrust laws where the defendant's name appears in the case title.

Categories of records in the system:

This system contains an index reference to the case in which an individual (or corporation) was a defendant; included information is proper case name, the judicial district, number of the case, the commodity involved, each alleged violation, the section of the Antitrust Division responsible for the matter, and the disposition of the case.

Authority for maintenance of the system:

Authority for maintaining this system exists under 44 U.S.C. 3101 and 28 U.S.C. 522.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

This index is maintained for ready reference by Department personnel. It is utilized for reference to case names, the preparation of speeches and to aid in determinations of the antitrust histories of companies.

A record maintained in this system, or any facts derived therefrom, may be disseminated in a proceeding before a court or adjudicative body before which the Antitrust Division is authorized to appear, when (1) the Antitrust Division, or any subdivision thereof; or (2) any employee of the Antitrust Division in his or her official capacity; or (3) any employee of the Antitrust Division in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (4) the United States, or any agency or subdivision thereof; or (5) the United States, where the Antitrust Division determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the Antitrust Division to be arguably relevant to the litigation.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 28 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional

licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information contained in this system is maintained on index cards.

Retrievability:

Information is retrieved by case name.

Safeguards:

Information contained in the system is unclassified. During duty hours access to this system is monitored and controlled by Antitrust Division personnel in the area where the system is maintained. This area is locked during non-duty hours.

Retention and disposal:

Indefinite.

System manager(s) and address:

Chief, Freedom of Information Act/Privacy Act Unit, Antitrust Division. U.S. Department of Justice, Liberty Place, Suite 200, Washington DC 20530.

Notification procedure:

Address inquiries to the Assistant Attorney General, Antitrust Division, U.S. Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Record access procedures:

Request for access to a record from this system should be made in writing and be clearly identified as a "Privacy Access Request." Included in the request should be the name of the defendant appearing in the title of the pending or terminated Government antitrust litigation. The Requester should indicate a return address. Requests will be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the index should direct their request to the System Manager and state clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to be information sought.

Record source categories:

Sources of information maintained in the index are those records reflecting litigation controlled by the Antitrust Division.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/ATR-009

System name:

Public Compliants and Inquiries File.

System location:

U.S. Department of Justice, Washington, DC 20530 and field office locations as follows:
Peachtree St., NW, Suite 420, Atlanta, GA 30309; 2634 Everett M. Dirksen Bldg., 219 S Dearborn St., Chicago, IL 60604; 995 Celebrezze Federal Bldg., 1240 E. 9th St., Cleveland, OH 44199; Earl Cabell Federal Bldg., Room 3101 Federal Bldg., Los Angeles, CA 90013; Room 3630, 26 Federal Plaza, New York, NY 10007; 3430 U.S. Courthouse, Independence

Mall West, 601 Market St., Philadelphia, PA 19106; and 450 Golden Gate Ave., Box 360
San Francisco, CA 94102.

Categories of individuals covered by the system:

Members of the public who submit unsolicited complaints and inquiries to the Division of
official business.

Categories of records in the system:

The file will contain letters or notes of other contacts by members of the public.

Authority for maintenance of the system:

The file will be established and maintained pursuant to 44 U.S.C. 3101 and 5 U.S.C. 30

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The file will be used by Antitrust Division personnel to assure adequate response to initial
subsequent contacts by the same individuals or to other contacts regarding the same subject.
Some of these contracts will also serve to further ongoing Antitrust investigations or to initiate
an investigation for enforcement purposes. Complaints/inquiries may be referred to other
federal or state and local agencies, only if deemed appropriate to assure complete action on
the matter.

Release of information to members of Congress: Information contained in systems of records
maintained by the Department of Justice, not otherwise required to be released pursuant to
U.S.C. 552, may be made available to a Member of Congress or staff acting upon the
Member's behalf when the Member or staff requests the information on behalf of and at the
request of the individual who is the subject of the record.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose
relevant and necessary information to a former employee of the Department for purposes of
responding to an official inquiry by a federal, state, or local government entity or professional
licensing authority, in accordance with applicable Department regulations; or facilitating
communications with a former employee that may be necessary for personnel-related or

official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records will be maintained in the form in which they are originated, i.e., paper letters, notes, and log sheets.

Retrievability:

Information will be retrieved by name, subject matter and date.

Safeguards:

Information contained in the system will be unclassified. Records will be maintained only in the offices of the Antitrust Division and accessed only by Division employees whose official duties require such access.

Retention and disposal:

Records of contacts will be kept by individual name for one year, after which they will be destroyed. Copies of these contact records may be placed in a subject matter or case file if they contain substantive information on antitrust enforcement matters. Case and subject matter files are normally maintained for thirty years.

System manager(s) and address:

Executive Officer, Antitrust Division, U.S. Department of Justice, Washington, DC 20530

Notification procedure:

Same as System Manager.

Record access procedures:

Same as Notification.

Contesting record procedures:

Same as Notification.

Record source categories:

All information will be obtained from the complaining individuals themselves.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/ATR-014

System name:

Civil Investigative Demand (CID) Tracking System, (JUSTICE/ATR-014).

System location:

Information Systems Support Group, Antitrust Division, Department of Justice, Judiciary Building, 555 4th Street, NW, Washington, DC 20001.

Categories of individuals covered by the system:

Recipients of Antitrust Division (ATD) CID's in connection with certain ATD civil investiga

Categories of records in the system:

The CID number, the name of the CID recipient, the name of the company that employs CID recipient, the date of CID, the type of CID (documentary, interrogatory or oral), the Department of Justice file number for the investigation and/or the title or subject of the investigation for which the CID was issued, and a reference indicating whether a matter

litigated as a result of information obtained by CID.

Authority for maintenance of the system:

The system is maintained pursuant to 28 U.S.C. 522, 44 U.S.C. 3101, and 28 CFR 0.40

Purpose(s):

The proposed system contains information relating to the issuance of CID's (CID's require production of documents and/or answers to written interrogatories, or oral testimony in connection with certain ATD civil investigations.) The system will be used by ATD to determine whether a party has been the recipient of a CID during a previous investigation(s), to identify the title (or nature) of that investigation(s), and to determine whether that individual should be issued a CID in an ongoing investigation(s).

Routine uses of records maintained in the system, including categories of users and purpose of such uses:

Where ATD has reason to believe that information from this system of records, e.g., names of individuals who are potential sources of information, may assist another agency (whether Federal, State, local or foreign) in the conduct of its investigation(s) the information may be disclosed to such agency to provide that agency with or to assist the agency in identifying essential investigative leads.

Records or information may be disclosed as a routine use in a proceeding before a court or adjudicative body before which the Department is authorized to appear when any of the following is a party to litigation or has an interest in litigation and such records are determined by the Department to be arguably relevant to the litigation: The Department or any of the Department's components or its subdivisions; any Department employee in his or her official capacity, or in his or her individual capacity where the Department of Justice agrees to represent the employee; or the United States where the Department determines that the litigation is likely to affect it or any of the Department's components or its subdivisions.

Records or information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Records or information may be disclosed as is necessary to respond to congressional inquiries on behalf of constituents.

Records may be disclosed to the National Archives and Records Administration (NARA) during the General Services Administration in records management inspections conducted under the authority of title 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

The records in this system are stored in a computer database.

Retrievability:

Records are retrieved by the name of the individual who has been issued a CID.

Safeguards:

The information stored on the computer database is password-protected. Passwords and ID's are issued to authorized ATD employees only on a need-to-know basis.

Retention and disposal:

Proposed plans for the retention and disposal of these records are being reviewed by the Department. Upon submission to and approved by the NARA, this system notice will be used to identify the appropriate General Records Schedule that will govern the disposition of

records.

System manager(s) and address:

The system manager is the Chief, Information Systems Support Group, Antitrust Division, Department of Justice, Judiciary Center Building, room 11852, 555 4th Street, NW, Washington, DC 20001.

Notification procedure:

Inquiries should be addressed to the Freedom of Information Act/Privacy Act (FOIA/PA) Antitrust Division, Department of Justice Liberty Place, Suite 200, Washington, DC 20533. Clearly mark the letter and envelop "FOIA/PA Request."

Record access procedures:

Make all requests for access in writing and clearly mark the letter and envelope "FOIA/PA Request." Clearly indicate the name of the requester, name of the individual for which information is sought and provide the required verification of identity (28 CFR 16.41(d)). Submit all requests to the FOIA/PA Officer listed above and provide a return address for transmitting the information.

Contesting record procedures:

Direct all requests to contest or amend information to the FOIA/PA Officer listed above. Clearly and concisely state the information being contested, the reason for contesting it, and the proposed amendment to the information sought. Clearly mark the letter and envelope "FOIA/PA Request."

Record source categories:

Employers of CID recipients, or other investigative sources, who may provide the names of potential CID recipients; the individuals covered by the system; and records generated in the virtue of the issuance of CID's.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

Board of Immigration Appeals

JUSTICE/BIA-001

System name: Decisions of the Board of Immigration Appeals.

System location:

5203 Leesburg Pike, Falls Church, Virginia 22041.

Categories of individuals covered by the system:

(a) Aliens, including those previously admitted for lawful permanent residence, in depor proceedings; (b) Aliens and alleged aliens in exclusion proceedings; (c) Aliens seeking of inadmissibility; (d) Aliens in bond determination proceedings; (e) Aliens in whose beh preference classification is sought.

Categories of records in the system:

This system of records consists of the formal orders and decisions of the Board of Immig Appeals, including the indices and logs pertaining thereto.

Authority for maintenance of the system:

This system is established and maintained under the authority granted the Attorney Ge sections 103 and 292 of the Immigration and Nationality Act, 8 U.S.C. 1103 and 1362. S authority has been delegated to the Board of Immigration Appeals by 8 CFR part 3.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The Decisions of the Board of Immigration Appeals are disseminated to the following ca of users for the purposes indicated:

(a) Parties appearing before the Board, (including the Immigration and Naturalization Service and their attorneys or other representatives. Purpose: Parties are entitled to the decision as a matter of due process; and in accordance with the requirements of 8 CFR 3.1(g).

(b) Other lawyers, organizations recognized to appear before the Immigration and Naturalization Service and their representatives. Purpose: To permit these users to be informed of current case law and general maintenance of open system of jurisprudence.

(c) Members of Congress. Purpose: Constituent inquiries.

(d) General public. Purpose: Selected decisions, designated as precedent decisions pursuant to 8 CFR are published in bound volumes of Administrative Decisions Under Immigration and Nationality Laws of the United States. These are published to provide the public with guidance on the administrative interpretation of the immigration laws and to facilitate open and uniform adjudication of cases.

Release of information to the news media:

Information permitted to be released to the news media and the public pursuant to 28 C.F.R. 50.2 may be made available from systems of records maintained by the Department of Justice, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress.

Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or

official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information in the system is kept in typed form and stored in loose leaf binders.

Retrievability:

Each decision is indexed by name and a numerical identifier.

Safeguards:

Information contained in the records is unclassified and intended for wide dissemination. Specific safeguards to prevent unauthorized disclosure are employed since no type of disclosure is presently regarded as "unauthorized". Access to buildings in which records are stored is controlled by guards provided by GSA.

Retention and disposal:

Records are retained indefinitely and are not disposed of.

System manager(s) and address:

Executive Assistant, Board of Immigration Appeals, Department of Justice, Washington, DC 20530.

Notification procedure:

Same as the above.

Record access procedures:

Decisions of the Board of Immigration Appeals are available to anyone upon request pursuant to the Freedom of Information Act.

to 5 U.S.C. 552a(b)(2).

Contesting record procedures:

Decisions of the Board of Immigration Appeals constitute official opinions and are not subject to correction or amendment except in accordance with accepted standards of due process. Decisions have been exempted from the correction provisions of 5 U.S.C. 552a(d).

Record source categories:

Sources of information contained in this system are provided primarily by the record of proceedings forwarded by the Immigration and Naturalization Service. Additionally, the individual concerned and his representative provide information.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsection (d)(2), (3) and (4) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/BIA-002

System name:

Roster of Organizations and their Accredited Representatives Recognized by the Board of Immigration Appeals.

System location:

5203 Leesburg Pike, Falls Church, Virginia 22041.

Categories of individuals covered by the system:

(a) Persons associated in an official capacity with a recognized organization; (b) Person

have applied for, have been granted or have been denied accreditation as representative recognized organizations.

Categories of records in the system:

This system consists of (a) a roster of charitable, social service and similar organizations of their accredited representatives; (b) applications and related documents submitted by organizations and their representatives and (c) orders of the Board of Immigration Appeals granting or denying recognition to such organizations and their representatives. Recognized organizations and their accredited representatives are authorized to practice before the Immigration and Naturalization Service and Board of Immigration Appeals.

Authority for maintenance of the system:

This system is established and maintained under the authority granted the Attorney General sections 103 and 292 of the Immigration and Nationality Act, 8 U.S.C. 1103 and 1362. Such authority has been delegated to the Board of Immigration Appeals by 8 CFR part 292.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Copies of decisions granting or denying applications for recognition and accreditation are made available to (a) the organization seeking recognition and (b) the Immigration and Naturalization Service.

Release of information to the news media:

Information permitted to be released to the news media and the public pursuant to 28 C.F.R. 50.2 may be made available from systems of records maintained by the Department of Justice, unless it is determined that release of the specific information in the context of a particular request would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information contained in the system is stored in file folders.

Retrievability:

Information is retrieved by use of the name of the organization or person accredited.

Safeguards:

Information contained in this record system is unclassified. Access to building in which records are stored is controlled by guards provided by GSA. No specific safeguards are employed.

Retention and disposal:

Records in this system are retained indefinitely.

System manager(s) and address:

Executive Assistant, Board of Immigration Appeals, Department of Justice, Washington, DC 20530.

Notification procedure:

Address inquiries to: Chairman, Board of Immigration Appeals, Department of Justice, Washington, DC 20530.

Record access procedures:

A request for access to a record from this system shall be made in writing, with the envelope and letter clearly marked "Privacy Access Request." Include in the request(s) the name of the organization which has sought, or has been granted or denied recognition and the name of the individual who has sought accreditation as a representative of such organization, or, where the organization is concerned, the name of the individual who has sought accreditation or recognition. The requester will provide a return address for transmitting the information. All requests will be directed to the System Manager listed above.

Contesting record procedures:

The procedures for contesting or amending information contained in this system of records are governed by 8 CFR part 292. The procedures require that organizations seeking accreditation and their representatives be notified of adverse information and be given an opportunity to contest such information.

Record source categories:

Sources of information contained in this system are supplied by the organization seeking recognition, individuals seeking accreditation, and reports supplied by the Immigration and Naturalization Service.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

Bureau of Prisons

JUSTICE/BOP-001

System name:

Prison Security and Intelligence Record System.

System location:

Records may be retained at any of the Bureau's facilities, the Regional Offices and the Office. A list of current addresses is contained in 28 CFR part 503 and on the Internet at <http://www.bop.gov>.

Categories of individuals covered by the system:

Current and former inmates under the custody of the Attorney General and/or the Director of the Bureau of Prisons.

Categories of records in the system:

Records in this system include:

(a) Identification information including name, register number (if an inmate), and fingerprint information; (b) Information concerning escape plots, assaults, and disturbances; (c) Investigative reports; (d) Intelligence information; (e) Confidential Informant information; (f) Referral records; (g) Telephone call records.

Authority for maintenance of the system:

This system is established and maintained under the authority of 18 U.S.C. 3621, 4042, 5003.

Purpose(s):

The records in this system are maintained to assist the Bureau in investigating and documenting inmate incidents and prison disturbances for purposes of guarding the safety of other inmates, Bureau staff and the general public. This system assists Bureau staff in gathering and organizing information on serious prison incidents such as escape plots, assaults, major prison disturbances, investigative reports and confidential informant information. This system is necessary to better ensure prison security and better protect inmates, staff and the public.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant data from this system may be disclosed as follows:

- (a) As permitted in the Privacy Act, 5 U.S.C. 552a(b)(1), to officers and employees of the Department of Justice who have a need for the information in the performance of their duties;
- (b) To federal, state, local, tribal, international and foreign law enforcement officials who need for the information to perform their duties e.g., in the course of apprehensions, investigations, possible criminal prosecutions, civil court actions, regulatory proceedings, inmate disciplinary hearings, parole hearings, responding to emergencies, or other law enforcement activity; information may also be disclosed to such law enforcement agency in order to solicit or obtain data needed by prison officials for law enforcement purposes;
- (c) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of an individual who is the subject of the record;
- (d) To the National Archives and Records Administration (NARA) and to the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;
- (e) In a proceeding before a court, grand jury, or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding;
- (f) To a federal, state, or local licensing agency or association which requires information concerning the suitability or eligibility of an individual for a license or permit;
- (g) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish a Bureau function related to this system of records;
- (h) To any person or entity to the extent necessary to prevent immediate loss of life or serious bodily injury;
- (i) Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose

relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored in electronic media in Bureau facilities via configuration of personal computer, client/server, and mainframe systems architecture. Computerized records are maintained on hard disk, floppy diskettes, magnetic tapes, compact discs (CDs) and/or optical disks. Documentary records are maintained in microfilm, manila folders and/or index card files.

Retrievability:

Records are retrievable by institution, date, type of incident, and, where available, by individual name.

Safeguards:

Information is safeguarded in accordance with Bureau rules and policy governing sensitive data and automated information systems security and access. These safeguards include maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Only those Bureau personnel who require access to perform their official duties may access the system equipment and the information in the system. Documentary records are maintained in secure areas locked, fireproof cabinets, in guarded buildings and accessed only by authorized personnel.

Retention and disposal:

Records in this system are retained for five (5) years after initial documentation of the incident and, if appropriate, may be incorporated into another system of records, e.g.

JUSTICE/BOP-005, Inmate Central Record System. Records concerning major prison disturbances are sent to the National Archives for permanent storage. Non-criminal activities are kept at the institution for five years, after which they are destroyed by shredding. Automated records are destroyed by degaussing.

System manager(s) and address:

Assistant Director, Correctional Programs Division, Federal Bureau of Prisons, 320 First NW., Washington, DC 20534.

Notification procedure:

Inquiries concerning this system should be directed to the System Manager listed above.

Record access procedure:

All requests for records may be made by writing to the Director, Federal Bureau of Prisons, First Street NW., Washington, DC 20534, and should be clearly marked "Privacy Act Request." This system is exempt, under 5 U.S.C. 552a (j), from some access. A determination as to whether an exemption shall be made at the time a request for access is received.

Contesting record procedures:

Same as above.

Record source categories:

Bureau staff, inmates, confidential informants, and law enforcement officials.

Systems exempted from certain provisions of the act:

Pursuant to 5 U.S.C. 552a(j), the Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(2) and (3), (e)(4)(H), (e)(8), (f), and (g). Rules have been promulgated in accordance with the requirement of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register* and codified at 28 CFR 16.97(a) and (b).

[\[TOP\]](#)

JUSTICE/BOP-003

System name:

Industrial Inmate Employment Record System.

System location:

Records may be retained at any of the Bureau's facilities, the Regional Offices and the Central Office. All requests for records may be made to the Central Office: U.S. Bureau of Prisons, 1015 First Street NW, Washington, DC 20534.

Categories of individuals covered by the system:

Current and former inmates under the custody of the Attorney General.

Categories of records in the system:

(1) Inmate assignment records; (2) Time and Attendance Reports; (3) Work Performance Reports; (4) Payroll Records.

Authority for maintenance of the system:

This system is established and maintained under authority of 31 U.S.C. 841; 18 U.S.C. 4121 et seq.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The routine uses of this system are: (a) To determine compensation of inmates pursuant to 18 U.S.C. 4002, 4126, 4125, 4121 et seq.; (b) to record employment history of an inmate with the Federal Prison Industries, Inc.; (c) to record disbursement of Federal Prison Industries, Inc., funds for payroll purposes; (d) to evaluate effectiveness of industrial training of inmates; (e) to evaluate authenticity of Federal Prison Industries, Inc., accounting records; (f) to provide information source to officers and employees of the Department of Justice who have need for information in the performance of their duties; (g) to provide information sources to state and federal law enforcement officials for investigations, possible criminal prosecution, civil cases.

actions, or regulatory proceedings; (h) to provide information relating to federal offender federal and state courts, court personnel, and probation officials.

Release of information to the news media: Information permitted to be released to news and the public pursuant to 28 CFR 50.2 may be made available from systems of record maintained by the Department of Justice unless it is determined that release of the specified information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations facilitating communications with a former employee that may be necessary for personnel related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored on documents, magnetic tape, magnetic tab cards, and microfilm.

Retrievability:

(1) Documents, Tab Cards and Microfilm—Information is indexed by name and/or register number. (2) Magnetic Tape and Disk—information is indexed by Name, Register Number, Social Security Number, and FBI Number.

Safeguards:

Information is safeguarded in accordance with Bureau of Prisons rule governing access release.

Retention and disposal:

Records in this system are retained for a period of thirty (30) years after expiration of sentence then destroyed by shredding.

System manager(s) and address:

Chief, Management and Information Systems Group, U.S. Bureau of Prisons, 320 First Street, NW, Washington, DC 20534.

Notification procedure:

Address inquiries to: Director, Bureau of Prisons, 320 First Street, NW, Washington, DC 20534. The major part of this system is exempt from this requirement under 5 U.S.C. 552a (j). If an inquiry concerning this system should be directed to the System Manager listed above.

Record access procedures:

The major part of this system is exempt from this requirement under 5 U.S.C. 552a (j). To the extent that this system of records is not subject to exemption, it is subject to access and contest. A determination as to exemption shall be made at the time a request for access is received.

Contesting record procedures:

Same as the above.

Record source categories:

(1) The inmate; (2) Bureau of Prisons/Federal Prison Industries staff members; (3) U.S. Treasury Department.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(3), (e)(4)(H), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/BOP-004

System name:

Inmate Administrative Remedy Record System.

System location:

Records may be retained at the Central Office, Regional Offices, or at any of the Federal Bureau of Prisons (Bureau) facilities, or at any location operated by a contractor authorized to provide computer and/or correctional services to Bureau inmates. A list of Bureau facilities can be found at 28 CFR part 503 and on the Internet at <http://www.bop.gov>.

Categories of individuals covered by the system:

Current and former inmates, including pre-trial detainees, under the custody of the Attorney General and/or the Director of the Bureau of Prisons.

Categories of records in the system:

Records in this system include: (1) Inmate information including (a) name; (b) registration number; (c) institution location; (d) current offense and sentence; (e) prior criminal record; (f) social background; (g) institution adjustment; (h) institution program data; (i) medical information.

(j) personal property data; (2) complaint information including copies of BOP–9's (institution level complaints), BOP–10's (Region appeals) and BOP–11's (Central Office appeals); and (3) processing information, including dates of filing and responses.

Authority for maintenance of the system:

The system is established and maintained under authority of 18 U.S.C. 3621, 4042, 5002 and 28 CFR part 542.

Purpose(s):

The Bureau maintains records of the receipt, processing and responses to grievances filed by inmates pursuant to the Bureau's Administrative Remedy Program, which was established to provide inmates with a means to seek formal review of issues relating to conditions of their confinement. The related uses for which the Bureau maintains the system include (1) to provide a source of information for reconsideration or amendment of Bureau policy with respect to its operation; (2) to maintain a source of information for purposes of defending civil actions filed against the Bureau by inmates; and (3) to provide a source of information for statistical reports furnished to federal courts for the purpose of determining exhaustion of administrative remedies and the effectiveness of the Administrative Remedy Program in reducing the number of cases filed in federal court.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant data from this system will be disclosed as follows:

(a) To federal, state, local, foreign and international law enforcement agencies and officials for law enforcement purposes such as civil court actions, regulatory proceedings, responding to an emergency, inmate disciplinary proceedings; or for such law enforcement needs as prison administration, investigations, and possible criminal prosecutions.

(b) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system's records;

- (c) To Members of Congress or staff acting upon the Member's behalf when the Member staff requests the information on behalf of and at the request of the record subject;
- (d) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;
- (e) To the National Archives and Records Administration and General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;
- (f) In a proceeding before a court, grand jury, or administrative or regulatory body when records are determined by the Department of Justice to be arguably relevant to the proceeding;
- (g) To a federal, state, or local licensing agency or association which requires information concerning the suitability or eligibility of an individual for a license or permit and;
- (h) Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of:
 - Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or
 - Facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored in electronic media via a configuration of personal computer, client/server, and mainframe systems architecture and may be accessed by only those staff with a need-to-know at all Bureau and contractor facilities. Some information may be stored in other computerized media, e.g., hard disk, floppy diskettes, magnetic digital recordings, Compact Discs (CDs), and/or optical disks. Documentary records are

maintained in manual file folders.

Retrievability:

Documents are indexed by name and/or register number.

Safeguards:

Automated information is safeguarded in accordance with Department of Justice and Bureau of Prisons rules and policy governing automated information systems security and access. Safeguards include the maintenance of records and technical equipment in restricted areas, e.g. controlled access buildings, and the required use of proper passwords and user identification codes to access the system. Manual records are stored in a file room. All records in Bureau facilities are maintained in guarded buildings.

Retention and disposal:

Case files, stored electronically and/or on paper, are maintained for a period of three (3) years from the date the response is completed, at which time they are destroyed. Indexes are maintained for a period of twenty (20) years, at which time they are destroyed.

System manager(s) and address:

Assistant Director/General Counsel, Federal Bureau of Prisons; 320 First Street NW., Washington, DC 20534.

Notification procedure:

Inquiries should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made by writing to the System Manager identified above at the Federal Bureau of Prisons, 320 First Street NW., Washington, DC 20534. The envelope must be clearly marked "Privacy Act Request." This system of records is exempted from access pursuant to 5 U.S.C. 552a(j). A determination as to the applicability of the exemption to any particular record(s) shall be made at the time a request for access is received.

Contesting record procedures:

Same as above.

Record source categories:

Records are generated by: Inmates; individuals covered by the system; Bureau staff; federal, state, local, tribal, and foreign law enforcement agencies; and federal/state probation and judicial offices.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(3), (e)(4)(H), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register* and codified at 28 CFR 16.97 (a) and (b).

[\[TOP\]](#)

JUSTICE/BOP-005

System name:

Inmate Central Records System.

System location:

Records may be retained at the Central Office, Regional Offices, or at any of the Federal Bureau of Prisons (Bureau) and/or contractor-operated correctional facilities. A list of Bureau locations may be found at 28 CFR part 503 and on the Internet at <http://www.bop.gov>.

Categories of individuals covered by the system:

Individuals currently or formerly under the custody of the Attorney General and/or the Department of Justice, Bureau of Prisons.

Categories of records in the system:

This system contains records relating to the care, classification, subsistence, protection discipline, and programs of federal inmates. Such records may include:

(1) Computation of sentence and supporting documentation; (2) correspondence and other documentation concerning pending charges, and wanted status, including warrants; (3) requests from other federal and non-federal law enforcement agencies for notification of release; (4) records of the allowance, forfeiture, withholding and restoration of good time; (5) information concerning present offense, prior criminal background, sentence and parole; (6) identification data including date of birth, Social Security number, driver's license number, registration number, physical description, sex, race, religious preference, photographs, fingerprints, digital image, biometric identifier, drug testing and DNA samples and analysis records; (7) institution designation and housing assignments, including separation orders and supporting documentation; (8) work and payroll records; (9) program selections, assignments and performance or progress reports; (10) prison conduct records, including information concerning disciplinary actions, participation in escapes, assaults, and disturbances; (11) economic, social, and religious background, including special religious dietary requirements; (12) educational data, including industrial and vocational training; (13) physical and mental health data; (14) United States Parole Commission orders, actions and related forms; (15) correspondence regarding the inmate, including his or her release, adjustment and violations; (16) transfer information, including orders and transportation arrangements; (17) mail, visitation and telephone records; (18) personal property records; (19) safety reports and rules; (20) release processing forms and certificates; (21) interview requests; (22) litigation related records; (23) investigatory information; (24) institution tracking records to locate archived records; (25) referrals of non-federal inmates to Bureau custody and/or referrals of Bureau inmates to state custody.

Authority for maintenance of the system:

This system is established and maintained under the authority of 18 U.S.C. 3621, 4042, (state inmates), and section 11201 of Chapter 1 of Subtitle C of Title XI of the National Corrections Revitalization and Self-Government Improvement Act of 1997 (Pub. L. 105-33; 111 Stat.

Purpose(s):

This system assists the Attorney General and the Bureau of Prisons in meeting statutory responsibilities for the safekeeping, care and custody of incarcerated persons. It serves

primary record system on these individuals and includes information critical to the continuing safety and security of federal prisons and the public.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant data from this system will be disclosed as follows:

(a) To officers and employees of the Bureau of Prisons and the Department of Justice who have a need for the information in the performance of their duties;

(b) To federal, state, local, tribal, foreign and international law enforcement agencies and officials for law enforcement and court-related purposes such as investigations, possible criminal prosecutions, civil court actions, or regulatory or parole proceedings, and, prior to the release of an inmate, to the chief law enforcement officer of the state and local jurisdiction in which the released inmate will reside, as required by 18 U.S.C. 4042(b);

(c) To a court or adjudicative body before which the Department of Justice or the Bureau is authorized to appear, or to a private attorney authorized by the Department of Justice to represent a Bureau employee, when any of the following is a party to litigation or has an interest in litigation and such records are determined by the Bureau to be arguably relevant to the litigation: (1) The Bureau, or any subdivision thereof, or the Department of Justice, or any Department of Justice or Bureau employee in his or her official capacity, or (3) any Department of Justice or Bureau employee in his or her individual capacity where the Department of Justice has agreed to provide representation for the employee, or (4) the United States, where the Bureau determines that the litigation is likely to affect it or any of its subdivisions;

(d) In an appropriate proceeding before a court or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding, including federal, state, and local licensing agencies or associations which disseminate information concerning the suitability or eligibility of an individual for a license or permit;

(e) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;

(f) To victims and/or witnesses, pursuant to federal victim/witness legislation and policy requiring the release of information relating to an inmate's furlough, parole (including appearance before the United States Parole Commission), transfer to a community correction center, mandatory release, expiration of sentence, escape (including apprehension), death and other such release-related information;

(g) To state agencies and authorities, pursuant to Public Law 98–135, for the purpose of matching the data against state records to review eligibility of these inmates for unemployment compensation; the requesting state is to erase the Bureau data after this determination has been made;

(h) To the Social Security Administration (SSA), pursuant to Public Law 96–473, for the purpose of matching the data against SSA records to enable the SSA to determine the eligibility of Bureau inmates to receive benefits under the Social Security Act and for the purpose of assisting SSA in providing inmate data to the states administering federal benefit programs such as Food Stamps; SSA is to erase the Bureau data after the match has been made;

(i) To the Veterans Administration (VA), pursuant to Public Law 96–385, for the purpose of matching the data against VA records to determine the eligibility of Bureau inmates to receive veterans' benefits; the VA is to erase the Bureau data after the match has been made;

(j) To the Federal Aviation Administration (FAA), pursuant to Public Law 100–690, for the purpose of matching the data against FAA records to determine the eligibility of Bureau inmates to hold and obtain airmen certification and qualification;

(k) To the Internal Revenue Service (IRS) for the purposes of matching the data against records for fraud detection;

(l) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(m) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record;

(n) To the National Archives and Records Administration and General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(o) To any person or entity to the extent necessary to prevent immediate loss of life or serious bodily injury;

(p) To a former employee of the Department, pursuant to subsection (b)(3) of the Privacy Act for purposes of: responding to an official inquiry by a federal, state, or local government or professional licensing authority, in accordance with applicable Department regulation facilitating communications with a former employee that may be necessary for personnel related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility; and

(q) To the United States Sentencing Commission (USSC) for the purpose of providing identification data to enable the USSC to perform research and conduct studies.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system: Storage:

Information maintained in the system is stored in electronic media in Bureau facilities via configuration of personal computer, client/server, and mainframe systems architecture. Computerized records are maintained on hard disk, floppy diskettes, Compact Discs (CDs), magnetic tapes and/or optical disks. Documentary records are maintained in microfilm, file folders and/or index card files.

Retrievability:

Records are retrievable by identifying data, including name, inmate register number, FE number, alien registration number and/or Social Security number.

Safeguards:

Information is safeguarded in accordance with Bureau rules and policy governing automated information systems security and access. These safeguards include the maintenance of

records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Only those Bureau personnel who require access to perform their official duties may access the system equipment and the information in the system.

Retention and disposal:

Records in this system are retained for a period of thirty (30) years after the expiration of a sentence. Records of an unsentenced inmate are retained for a period of ten (10) years after the inmate's release from confinement. Documentary records are destroyed by shredding; computer records are destroyed by degaussing and/or shredding.

System manager(s) and address:

Assistant Director, Correctional Programs Division, Federal Bureau of Prisons, 320 First Street NW, Washington, DC 20534.

Notification procedure:

Inquiries concerning this system should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made in writing to the Director, Federal Bureau of Prisons, 320 First Street NW., Washington, DC 20534, and should be clearly marked "Privacy Act Request." This system is exempt, under 5 U.S.C. 552a(j), from some access. To the extent that this system of records is not subject to exemption, it is subject to access and contest. A determination as to exemption shall be made at the time a request for access is received.

Contesting record procedures:

Same as above.

Record source categories:

Records are generated by: (1) Individual currently or formerly under custody; (2) federal, state, local, foreign and international law enforcement agencies and personnel; (3) federal and

prosecutors, courts and probation services; (4) educational institutions; (5) health care providers; (6) relatives, friends, and other interested individuals or groups in the community; (7) former or future employers; (8) state, local and private corrections staff; and (9) Bureau and institution contractors and volunteers.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(2), (e)(3), (e)(4)(H), (e)(5), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(b)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (e).

[\[TOP\]](#)

JUSTICE/BOP-006

System name:

Inmate Trust Fund Accounts and Commissary Record System.

System location:

Records may be retained at the Central Office, Regional Offices, or at any of the Federal Bureau of Prisons (Bureau) facilities, or at any location operated by a contractor authorized to provide computer, financial and/or correctional services to the Bureau. A list of Bureau facilities may be found at 28 CFR part 503 and on the Internet at <http://www.bop.gov>.

Categories of individuals covered by the system:

Individuals currently or formerly under the custody of the Attorney General and/or the Department of the Bureau of Prisons, vendors who supply products to institution commissaries, and persons who send or receive funds to/from inmates.

Categories of records in the system:

Records in this system include: (1) Financial data on individuals currently or formerly under custody; (2) personal identification data for individuals covered by this system; (3) vendor

and linked product information; and (4) system generated reports, such as Inmate Balance Reports, Transaction Input Listings, Inmate Sales Receipts, and Stock Status Reports.

Authority for maintenance of the system:

This system is established and maintained under authority of 18 U.S.C. 3621, 4042, and 31 U.S.C. 1321.

Purpose(s):

The purpose of this system is to track trust fund accounts of current and former inmates including all payments in and out of these accounts, to provide accounting of inmate trust balances for purposes of verifying pauper status under 28 U.S.C. 1915, and to maintain information on all vendors who supply products to institution commissaries to facilitate cost of commissary products.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant data from this system will be disclosed as follows:

- (a) To officers and employees of the Department of Justice who have a need for the information in the performance of their official duties;
- (b) To federal, state, local, tribal, foreign and international law enforcement agencies and officials for law enforcement purposes such as investigations, possible criminal prosecution, civil court actions, or regulatory proceedings;
- (c) To a court or adjudicative body before which the Department of Justice or the Bureau is authorized to appear for purposes of verifying pauper status under 28 U.S.C. 1915, or where any of the following is a party to litigation or has an interest in litigation and such record is determined by the Bureau to be arguably relevant to the litigation: (1) The Bureau, or any subdivision thereof, or (2) any Department or Bureau employee in his or her official capacity; (3) any Department or Bureau employee in his or her individual capacity where the Department has agreed to provide representation for the employee, or (4) the United States, where the Bureau determines that the litigation is likely to affect it or any of its subdivisions;

(d) In an appropriate proceeding before a court or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding, including federal, state, and local licensing agencies or associations which information concerning the suitability or eligibility of an individual for a license or permit;

(e) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(f) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record;

(g) To the National Archives and Records Administration and General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(h) To any person or entity to the extent necessary to prevent immediate loss of life or serious bodily injury;

(i) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system's records; and

(j) Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored in electronic media, including the Federal Point of Sale (FPPOS) System, in Bureau and contractor facilities via a configuration of personal computer, client/server, and mainframe systems architecture. Computerized records are maintained on hard disk, floppy diskettes, Compact Discs (CDs), magnetic tapes and optical disks. Documentary records are maintained in manual file folders and/or index card files.

Retrievability:

Records are retrievable by identifying data of the persons covered by the system, including name and address, inmate register number, and/or system-generated vendor number.

Safeguards:

Information is safeguarded in accordance with Bureau rules and policy governing automatic information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Only those Bureau and contractor personnel who require access to perform their official duties may access the system equipment and the information in the system.

Retention and disposal:

Inmate financial data in the system of records is retained for six years from the date of transaction, and system-generated reports are retained for as long as they are needed. Computerized records are destroyed by degaussing; documentary records are destroyed by shredding.

System manager(s) and address:

Chief, Trust Fund Branch, Administration Division, Federal Bureau of Prisons, 320 First NW., Room 5005, Washington, DC 20534.

Notification procedure:

Inquiries concerning this system should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made in writing to the Director, Federal Bureau of Prisons, First Street NW., Washington, DC 20534, and should be clearly marked "Privacy Act Request." This system is exempt, under 5 U.S.C. 552a (j) from some access. To the extent that this system of records is not subject to exemption, it is subject to access and contest. A determination as to exemption shall be made at the time a request for access is received.

Contesting record procedures:

Same as above.

Record source categories:

Records are generated by individuals currently or formerly under custody, persons sending or receiving funds to/from inmates, vendors supplying products to institution commissaries, Department of Justice and contractor employees.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(2), (e)(3), (e)(4)(H), (e)(5), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (e).

[\[TOP\]](#)

JUSTICE/BOP-007

System name:

Inmate Physical and Mental Health Record System.

System location:

Records may be retained at the Central Office, Regional Offices, or at any of the Federal Bureau of Prisons (Bureau) or at any location operated by a contractor authorized to provide correctional, medical, and/or computer service to the Bureau. A list of Bureau system locations may be found at 28 CFR part 503 and on the Internet at <http://www.bop.gov>.

Categories of individuals covered by the system:

Individuals currently or formerly under the custody of the Attorney General and/or the Director of the Bureau of Prisons.

Categories of records in the system:

Records in this system include: (1) Identification data, including name, inmate register number, date of birth, Social Security number, FBI number, drug testing and DNA samples and analysis; (2) medical and dental history and examinations (past and present), including diagnosis and treatment notes, records, and pharmaceutical information; (3) medical information concerning deaths of inmates; (4) offense information, including Pre-sentence Reports; (5) designations of inmates from parent facilities to medical facilities, including and type of referral; (6) pre-certifications authorizing inmates to receive care at local medical facilities, including authorized and actual length of stay, and all associated cost information; (7) mental health and drug abuse information, including interview, testing data, and progress observation notes, generated and maintained by Bureau staff; (8) mental health and drug abuse information generated outside the Bureau by other corrections agencies and health providers such as surgical clinics, mental hospitals, private therapists, etc.; (9) urine surveillance reports of drug program participants; (10) automated data, including Electronic Signatures, Sensitive Medical Data (SMD), Medical Duty Status (MDS), and Diagnosis Codes (DGN); and (11) information concerning infectious diseases, including HIV and Tuberculosis (TB) testing and treatment records.

Authority for maintenance of the system:

This system is established and maintained under the authority of 18 U.S.C. 3621, 4014, 4082, 4241 et seq., 5003, and section 11201 of Chapter 1 of Subtitle C of Title XI of the National Capital Revitalization and Self-Government Improvement Act of 1997.

Purpose(s):

This system assists the Bureau in providing appropriate health care to persons in the custody of the Bureau. It provides for the maintenance and release of records concerning the mental and dental health of persons in the Bureau's custody.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant data from this system will be disclosed as follows:

- (a) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;
- (b) To community health care professionals, including physicians, psychiatrists, psychologists, and federal medical facility personnel, who are providing treatment for a pre-existing condition to former federal inmates;
- (c) To federal, state, local, foreign and international law enforcement agencies and official law enforcement purposes such as investigations, possible criminal prosecutions, civil actions, or regulatory proceedings;
- (d) To a court or adjudicative body before which the Department of Justice or the Bureau is authorized to appear when any of the following is a party to litigation or has an interest in litigation and such records are determined by the Bureau to be arguably relevant to the litigation: (1) The Bureau, or any subdivision thereof, or (2) any Department or Bureau employee in his or her official capacity, or (3) any Department or Bureau employee in his or her individual capacity where the Department has agreed to provide representation for the employee, or (4) the United States, where the Bureau determines that the litigation is likely to affect it or any of its subdivisions;
- (e) In an appropriate proceeding before a court or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding, including federal, state, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit;

(f) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(g) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record;

(h) To the National Archives and Records Administration and General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(i) To any person or entity to the extent necessary to prevent immediate loss of life or serious bodily injury; and

(j) For information relating to infectious diseases, as follows:

(1) To state health departments and/or the Center for Disease Control, pursuant to state or federal laws requiring notice of cases of reportable infectious diseases;

(2) To the United States Probation Office in the district where an inmate is being released from Bureau custody on parole, placement in a community-based program, furlough, or full-time release, when the inmate is known to be HIV positive or under treatment for exposure to active Tuberculosis (TB);

(3) To the Director of a Community Corrections Center (halfway house) receiving an inmate from Bureau custody when the inmate is known to be HIV positive or under treatment for exposure to or active TB;

(4) To the physician/provider of a Bureau or non-Bureau staff, or other person exposed to blood-borne pathogen while lawfully present in a Bureau facility, for the purpose of providing prophylaxis or other treatment and counseling; and

(k) Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional

licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored in electronic media in Bureau facilities via configuration of personal computer, client/server, and mainframe systems architecture. Computerized records are maintained on hard disk, Compact Discs (CDs), floppy diskette, magnetic tapes and/or optical disks. Documentary records are maintained in manual file folders, microfilm and/or index card files.

Retrievability:

Records are retrievable by identifying data, including last name and inmate register number and/or the inmate's social security number and/or FBI number.

Safeguards:

Information is safeguarded in accordance with Bureau rules and policy governing automatic information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper password and user identification codes to access the system. Only those Bureau personnel who require access to perform their official duties may access the system equipment and the information in the system.

Retention and disposal:

Records in this system are retained for a period of thirty (30) years after expiration of the sentence. Documentary records are destroyed by shredding; computer records are destroyed by degaussing and/or shredding.

System manager(s) and address:

Assistant Director, Health Services Division, Federal Bureau of Prisons; 320 First Street
Washington, DC 20534.

Notification procedure:

Inquiries concerning this system should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made in writing to the Director, Federal Bureau of Prisons, 320 First Street NW., Washington, DC 20534, and should be clearly marked "Privacy Act request." This system is exempt, under 5 U.S.C. 552a(j), from some access. To the extent that this system of records is not subject to exemption, it is subject to access and contest. A determination as to exemption shall be made at the time a request for access is received.

Contesting record procedures:

Same as the above.

Record source categories:

Records are generated by: (1) Individuals currently or formerly under Bureau custody; (2) Bureau of Prisons staff; (3) community health care providers, including individuals, hospitals and/or other professionals involved in the medical, mental, and dental care of inmates and former inmates; and (4) other federal and/or state, local or tribal agencies, including those preparing or providing information on pre-sentence reports.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(2), (e)(3), (e)(4)(H), (e)(5), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(b)(7)(D). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (e).

[\[TOP\]](#)

JUSTICE/BOP-008

System name:

Inmate Safety and Accident Compensation Record System.

System location:

Records may be retained at the Central Office, Regional Offices, or at any of the Federal Bureau of Prisons (Bureau) facilities, or at any location operated by a contractor authorized to provide computer and/or correctional service to Bureau inmates. A list of Bureau facilities may be found at 28 CFR part 503 and on the Internet at <http://www.bop.gov>.

Categories of individuals covered by the system:

Current and former inmates, including pre-trial detainees, under the custody of the Attorney General and/or the Director of the Bureau of Prisons.

Categories of records in the system:

Records in this system include (a) inmate identification data including name, register number, location; (b) information concerning inmate accident/injuries sustained during : (1) Work related accidents; (2) recreation; (3) vehicle accidents; (4) assaults; and (5) other non-work-related accidents; and (c) processing data including dates of receipt of claims and responses.

Authority for maintenance of the system:

The system is established and maintained under authority of 18 U.S.C. 3621, 4042, 4125, and 5003.

Purpose(s):

This system of records is maintained to assist in the processing of inmate claims for injuries sustained during (1) work related accidents; (2) recreation; (3) vehicle accidents; (4) assaults; and (5) other non-work-related accidents. In addition, this system provides: (a) Documentation of inmate accidents and injuries for the purpose of measuring safety programs' effectiveness; (b) an information source of compliance with the Occupational Safety and Health Act; (c) documented records of inmate accidents, injuries, and disabilities for adjudicating claims by inmates filed under the Inmate Accident Compensation System established p

to 18 U.S.C. 4126 and regulations contained in 28 C.F.R. Part 301; and (d) background information and litigation reports to United States Attorneys for purpose of defending civil actions filed against the Bureau.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant data from this system may be disclosed as follows:

(a) To federal, state, local, foreign and international law enforcement agencies and official law enforcement purposes such as civil court actions, regulatory proceedings, responding to an emergency, inmate disciplinary proceedings; or for such law enforcement needs as prison administration, investigations, and possible criminal prosecutions;

(b) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;

(c) To Members of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the record subject;

(d) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(e) To consultant physicians treating inmates following release from custody for the purpose of providing medical history in conjunction with further treatment of the individual inmate;

(f) To the National Archives and Records Administration and General Services Administration for records management inspections conducted under the authority of 44 U.S.C. 2904 and

(g) In a proceeding before a court, grand jury, or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding;

(h) To a federal, state or local licensing agency or association which requires information

concerning the suitability or eligibility of an individual for a license or permit;

(i) Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored in electronic media via a configuration of personal computer, client/server, and mainframe systems architecture and may be accessed by those with a need-to-know at all Bureau and contractor facilities. Some information is also stored in other computerized media, e.g., hard disk, floppy diskettes, magnetic tape, digital recordings, Compact Discs (CDs), and/or optical disks. Documentary records are maintained in manual file folders and/or on index card files.

Retrievability:

Records may be retrieved by identifying data including name and/or register number of the record and/or claim number generated by the system.

Safeguards:

Manual records are stored in locked filing cabinets or in safes and can be accessed only by authorized personnel by key or combination formula. Automated equipment is kept in secure rooms and can be accessed only by authorized personnel through passwords and identification codes. All records in Bureau facilities are maintained in guarded buildings.

Retention and disposal:

Records in this system are retained for a period of two (2) years after expiration of sentence.

Some records may be transferred into another record system: the Inmate Central Record System, JUSTICE/BOP-005, or the Inmate Physical and Mental Health Record System, JUSTICE/BOP-007, and some records may be destroyed by shredding and/or electronic means.

System manager(S) AND ADDRESS:

Assistant Director, Health Services Division, Federal Bureau of Prisons; 320 First Street Washington, DC 20534.

Notification procedure:

Inquiries should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made by writing to the System Manager identified above: Federal Bureau of Prisons, 320 First Street NW., Washington, DC 20534. The envelope be clearly marked "Privacy Act Request." This system of records is exempted from access pursuant to 5 U.S.C. 552a(j). A determination as to the applicability of the exemption to particular record(s) shall be made at the time a request for access is received.

Contesting record procedures:

Same as above.

Record source categories:

Records are generated by: Individuals covered by the system (inmates and former inmates); Bureau staff; hospital and/or medical sources; pre-sentence reports; other mental health agencies' observation reports; Federal, State, local, tribal, and foreign law enforcement agencies; and Federal/State probation and judicial offices.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(3), (e)(4)(H), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j). Rules

been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register* and codified at 28 CFR 16.97(a) and (b).

[\[TOP\]](#)

JUSTICE/BOP-009

System name:

Administrative Claims Record System.

System location:

Records may be retained at the Central Office, Regional Offices, or at any of the Federal Bureau of Prisons (Bureau) facilities, or at any location operated by a contractor authorized to provide computer and/or correctional services to Bureau inmates. A list of Bureau facilities may be found at 28 CFR part 503 and on the Internet at <http://www.bop.gov>.

Categories of individuals covered by the system:

Current and former inmates, including pre-trial detainees, under the custody of the Attorney General and/or the Director of the Bureau of Prisons, civilians who are claimants under the Federal Tort Claims Act (FTCA), current and former employees who are claimants under the FTCA, the Military Personnel and Civilian Employees Claims Act (CECA), and the Bureau of Prisons Claims (BOPCA).

Categories of records in the system:

Records in this system include: (1) Claims and supporting documents; (2) personal data regarding the claimant, including name, register number (if an inmate or former inmate), address, social and criminal background (if applicable), and employment history; (3) investigative reports; (4) medical reports; (5) property records; (6) litigation reports, plea agreements and decisions; (7) correspondence; and (8) processing data, including dates of receiving and responding to the claim.

Authority for maintenance of the system:

The system is established and maintained under authority of the Federal Tort Claims Act.

U.S.C. 2671 et seq. (FTCA); the Military Personnel and Civilian Employees Claims Act, 38 U.S.C. 3721 (CECA); and the Bureau of Prisons Claims Act, 31 U.S.C. 3722 (BOPCA).

Purpose(s):

The purpose of this system is to process and track administrative claims submitted to the Bureau under the FTCA, the CECA, and the BOPCA. The system is maintained to assist in the processing of these claims for personal injury and/or property damages and to provide a ready information source for subsequent litigation concerning these claims in United States Courts.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant data from this system will be disclosed as follows:

- (a) To Federal, State, local, foreign and international law enforcement agencies and officials for law enforcement purposes such as civil court actions, regulatory proceedings, responding to an emergency, inmate disciplinary proceedings; or for such law enforcement needs as prison administration, investigations, and possible criminal prosecutions.
- (b) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;
- (c) To Members of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the record subject;
- (d) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;
- (e) To the National Archives and Records Administration and General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;
- (f) In a proceeding before a court, grand jury, or administrative or regulatory body when

records are determined by the Department of Justice to be arguably relevant to the proceeding;

(g) To a federal, state, or local licensing agency or association which requires information concerning the suitability or eligibility of an individual for a license or permit;

(h) Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility and

(i) To any person or entity to the extent necessary to prevent an immediate loss of life or serious bodily injury.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored in electronic media via a configuration of personal computer, client/server, and mainframe systems architecture and may be accessed by those with a need-to-know at all Bureau and contractor facilities. Some information is also stored in other computerized media, e.g., hard disk, floppy diskettes, magnetic tape, digital recordings, Compact Discs (CDs), and/or optical disks. Documentary records are maintained in manual file folders and/or on index card files.

Retrievability:

Documents are indexed by the claimant's name and/or claim number.

Safeguards:

Information is safeguarded in accordance with Bureau rules and policy governing automatic

information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas and the proper use of passwords and identification codes to access the system. Automated equipment and manual records are stored in guarded buildings and can be accessed only by authorized personnel through passwords and identification codes.

Retention and disposal:

Information in this system is maintained for twelve (12) years after close of case, at which time documentary records are destroyed by shredding. Electronic records are erased after ninety (90) days unless archived into the case file.

System manager(s) and address:

Assistant Director/General Counsel, Federal Bureau of Prisons; 320 First Street NW., Washington, DC 20534.

Notification procedure:

Inquiries should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made by writing to the System Manager identified above at the Federal Bureau of Prisons, 320 First Street NW., Washington, DC 20534. The envelope must be clearly marked "Privacy Act Request." This system of records is exempted from access pursuant to 5 U.S.C. 552a(j). A determination as to the applicability of the exemption to any particular record(s) shall be made at the time a request for access is received.

Contesting record procedures:

Same as above.

Record source categories:

Records are generated by: claimants; inmates; Bureau staff; Federal, State, local, tribal and foreign law enforcement agencies; Federal/State probation and judicial offices; Congress

contract and consulting physicians, including hospitals; and attorneys for claimants.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(3), (e)(4)(H), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register* and codified at 28 CFR 16.97(a) and (b).

[\[TOP\]](#)

JUSTICE/BOP-010

System name:

Access Control Entry/Exit System.

System location:

Records may be retained at the Central Office, Regional offices, and at any of the Bureau Prisons (Bureau) facilities. A list of these system locations may be found at 28 CFR part 16.97 and on the Internet at <http://www.bop.gov>.

Categories of individuals covered by the system:

Current and former staff, inmates now or formerly under the custody of the Attorney General, the Bureau, and all visitors to Bureau facilities, including law enforcement personnel, contractors, volunteers, and inmate visitors.

Categories of records in the system:

Information retrieved and stored by the system may include any information relative to providing safe and secure prison facilities, to protecting the prison population and/or the general public, and/or, where appropriate, to otherwise promoting the interests of effective law enforcement.

Examples include:

(a) Identification data (much of which is collected from the individual), such as the person's name, current residence, social security number, employer, place and date of birth, age, height, weight, digital image, biometric identifier information, alien registration number, driver's license number, telephone number, passport number, system-generated number, hair color, eye color, sex, race, escort of visitor into institution, and system classification of individual;

(b) Other data collected from the visitor and/or from law enforcement to enable prison officials to determine the suitability/acceptability of a visitor such as: the purpose of the visit, test results data regarding drugs, explosives, weapons and/or other contraband, relationship to the inmate, and information indicating whether the visitor is under investigation by law enforcement, whether the visitor has ever been convicted of a crime, probation and/or parole status, name of supervising probation/parole officer, etc.;

(c) Records generated by the system to report entry/exit activity, e.g. date and time of entry/exit, entry/exit locations used; and location data, including location in the institution visited and/or movement within the institution;

(d) Any related law enforcement or investigatory data, provided by third parties such as courts, inmates, courts, and other federal, state, local, and foreign law enforcement agencies, criminal history and/or investigatory data relating to potential visitors; investigatory data otherwise developed by Bureau officials regarding any activity, or suspicious activity, which may threaten the safe and secure operation of federal correctional facilities, e.g. remark describing a possible introduction of contraband; drug testing data; and any other information that may enable the Bureau to pursue an internal investigation on a record subject.

Authority for maintenance of the system:

This system is established and maintained under the authority of 18 U.S.C. 3621, 4042,

Purpose(s):

The records in this system are maintained to better ensure the safety, security and good order of Bureau facilities; to improve staff ability to quickly account for all persons (inmates, visitors and staff) within an institution in the event of an emergency, such as an institution disturbance or a natural disaster; to identify and, where appropriate, determine the suitability of visitors with respect to entering prison facilities; and, to more effectively prevent violations of institutional

policy and/or criminal activity, such as inmate escapes and the introduction of contraband. Where these efforts fail to prevent such violations, and/or where appropriate, records may be collected and used by the Bureau for internal investigations.

Routine uses of records maintained in the system, including categories of users and PURPOSE OF SUCH USES:

Relevant data from this system will be disclosed as follows:

- (a) To federal, state, local, foreign and international law enforcement agencies who have a need for the information to perform their duties, e.g. in the course of apprehensions, investigations, possible criminal prosecutions, civil court actions, regulatory proceedings, inmate disciplinary hearings, parole hearings, responding to emergencies, or other law enforcement activity;
- (b) To federal, state, local, foreign and international law enforcement agencies in order to obtain data needed by prison officials for law enforcement purposes, e.g. to determine whether a visitor may be under investigation, have a criminal record, or otherwise be unfit to visit; or to obtain any information that may enable the Bureau to pursue an internal investigation pertaining to any record subject based on information developed by the Bureau;
- (c) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;
- (d) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record;
- (e) To the National Archives and Records Administration (NARA) and to the General Services Administration in records management inspections conducted under the authority of 44 CFR 2904 and 2906;
- (f) To a court or adjudicative body before which the Department of Justice or the Bureau is authorized to appear when any of the following is a party to litigation or has an interest in litigation and such records are determined by the Bureau to be arguably relevant to the litigation: (1) The Bureau, or any subdivision thereof, or (2) any Department or Bureau

employee in his or her official capacity, or (3) any Department or Bureau employee in his or her individual capacity where the Department has agreed to provide representation for the employee, or (4) the United States, where the Bureau determines that the litigation is likely to affect it or any of its subdivisions;

(g) In an appropriate proceeding before a court or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding, including federal, state, and local licensing agencies or associations which maintain information concerning the suitability or eligibility of an individual for a license or permit;

(h) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;

(i) To any person or entity to the extent necessary to prevent immediate loss of life or serious bodily injury; and

(j) Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored in electronic media in Bureau facilities via the configuration of personal computer, client/server, and mainframe systems architecture. Computerized records are maintained on hard disks, floppy diskettes, compact discs (CDs), magnetic tape and/or optical disks. Documentary records are maintained in manual file folders and/or index card files.

Retrievability:

Records are retrievable by identifying data, including last name, inmate register number, system classification category, Social Security number, alien registration number, system-generated identification number, passport number, employee badge number and/or miscellaneous identification number as provided by the visitor and/or other law enforcement agencies.

Safeguards:

Information is safeguarded in accordance with Bureau rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Similarly, paper records are stored in secured areas to prevent unauthorized access. Only those Bureau personnel who require access to perform their official duties may access the records described in this system of records.

Retention and disposal:

Records generated by the system to report entry/exit and internal movement activities are retained in accordance with General Records Schedule (GRS) 18. All other records in the system of records are retained until such time as the records no longer serve the purpose described by this system of records. At such time, these records (including investigatory records and/or records relating to disciplinary hearings and/or other appropriate personnel actions) may be incorporated into an appropriate, published BOP system of records with approved retention schedule, or destroyed. Computerized records are destroyed by shredding, degaussing, etc., and documentary records are destroyed by shredding.

System manager(s) and address:

Assistant Director, Information, Policy, and Public Affairs Division, Federal Bureau of Prisons
320 First Street NW., Washington, DC 20534.

Notification procedure:

Inquiries concerning this system should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made by writing to the Director, Federal Bureau of Prisons, First Street NW., Washington, DC 20534, and should be clearly marked "Privacy Act Request." This system is exempt, under 5 U.S.C. 552a (j)(2) or (k)(2), from some access. A determination as to exemption shall be made at the time a request for access is received.

Contesting record procedures:

Same as above.

Record source categories:

Records are generated by: (1) Individuals covered by the system; (2) federal, state, local, foreign and international law enforcement agencies; and (3) federal and state probation and judicial offices.

System exempted from certain provisions of the act:

Pursuant to 5 U.S.C. 552a(j)(2) or (k)(2), the Attorney General has exempted this system from subsections (c)(3) and (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(5) and (e)(8), and (g) of the Privacy Act. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 552a(b)(5) and (e) and may be found at 28 CFR part 16.97 (c) and (d).

[\[TOP\]](#)

JUSTICE/BOP-011

System name:

Telephone Activity Record System.

System location:

Records may be retained at the Central Office, Regional Offices, or at any of the Federal Bureau of Prisons (Bureau) facilities, or at any location operated by a contractor authorized to provide computer and/or telephone service to Bureau inmates. A list of Bureau facilities

found at 28 CFR part 503 and on the Internet at <http://www.bop.gov>.

Categories of individuals covered by the system:

Current and former inmates, including pre-trial detainees, under the custody of the Attorney General and/or the Director of the Bureau of Prisons; recipients of telephone calls from and former inmates; individuals on the approved telephone lists of current or former inmates; individuals who request, in writing, that the Bureau delete their name and telephone number from inmate telephone lists.

Categories of records in the system:

Records in this system include: (1) Personal identification data; (2) accounting data, including amounts deposited by the inmate, call charges, and account balances; (3) telephone call records including date, time, and duration of each call; the name and register number of the inmate who placed the call; and the telephone number and name of the call recipient and his/her relationship to the inmate, audiotapes and digital recordings of telephone calls; and (4) investigatory data developed internally as well as any related data collected from federal, local and foreign law enforcement agencies, and from federal and state probation and parole officers.

Authority for maintenance of the system:

18 U.S.C. 2510 et seq., 3621, 4042, and 5003.

Purpose(s):

This system of records is maintained to manage financial records relating to inmate calls; ensure that inmates exercise their telephone privileges in a manner consistent with correctional goals. The related uses for which BOP will maintain the system include (1) accounting of inmate funds for telephone use; (2) maintaining inmate telephone lists; (3) monitoring of telephone activity; and (4) conducting investigations, e.g., investigation of inmate funds related to telephone usage, and/or illegal activities or suspected illegal activities being conducted, coordinated, or directed from within a federal correctional institution.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant data from this system will be disclosed as follows:

(a) To federal, state, local, foreign and international law enforcement agencies and official law enforcement purposes such as civil court actions, regulatory proceedings, responding to an emergency, inmate disciplinary proceedings in the course of apprehensions or other disposition; or for such law enforcement needs as prison administration, investigations, possible criminal prosecutions, including possible criminal violations discovered as part of telephone monitoring done for the safety, security and good order of penal institutions. Telephone monitoring information will be disclosed only in accordance with the provisions of federal wiretap statutes contained in 18 U.S.C. 2510 et seq. and Bureau implementing regulations.

(b) To a court or adjudicative body before which the Department of Justice or the Bureau is authorized to appear, or to a private attorney authorized by the Department of Justice to represent a Bureau employee, when any of the following is a party to litigation or has an interest in litigation and such records are determined by the Bureau to be arguably relevant to the litigation: (1) The Bureau, or any subdivision thereof, or (2) any Department or Bureau employee in his or her official capacity, or (3) any Department or Bureau employee in his or her individual capacity where the Department has agreed to provide representation for the employee, or (4) the United States, where the Bureau determines that the litigation is likely to affect it or any of its subdivisions;

(c) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;

(d) To Members of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the record subject;

(e) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(f) To the National Archives and Records Administration and General Services Administration for records management inspections conducted under the authority of 44 U.S.C. 2904 and

(g) To affected non-inmate record subjects to the extent necessary to provide such persons with information concerning placement and/or removal from an inmate's telephone list;

(h) To any person or entity to the extent necessary to prevent immediate loss of life or serious bodily injury;

(i) In an appropriate proceeding before a court or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding, including federal, state, and local licensing agencies or associations which disseminate information concerning the suitability or eligibility of an individual for a license or permit,

(j) Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored in electronic media via a configuration of personal computer, client/server, and mainframe systems architecture and may be accessed by those with a need-to-know at all Bureau and contractor facilities. Some information is also stored in other computerized media, e.g., hard disk, floppy diskettes, magnetic tape, digital recordings, Compact Discs (CDs), and/or optical disks. Documentary records are maintained in manual file folders and/or on index card files.

Retrievability:

Records may be retrieved by identifying data including name and/or register number of inmate and /or by name and/or telephone number of call recipient or individual on approved inmate telephone list.

Safeguards:

Manual records are stored in locked filing cabinets or in safes and can be accessed only by authorized personnel by key or combination formula. Automated equipment is kept in secure rooms and can be accessed only by authorized personnel through passwords and identification codes. All records in Bureau facilities are maintained in guarded buildings.

Retention and disposal:

With the exception of audiotapes and digital recordings, automated records in this system are maintained on magnetic medium ordinarily for six years from the date created, at which time they will be overwritten with new data. Paper documents are maintained for a period of 10 years from expiration of sentence of the inmate, at which time they are destroyed by shredding. Audiotapes and digital recordings are maintained ordinarily for six months from the date created, at which time they are overwritten with new data.

System manager(s) and address:

Assistant Director, Administration Division, Federal Bureau of Prisons; 320 First Street NW, Washington, DC 20534.

Notification procedure:

Inquiries should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made by writing to the System Manager identified above at the Federal Bureau of Prisons, 320 First Street NW, Washington, DC 20534. The envelope must be clearly marked "Freedom of Information/Privacy Act Request." This system of records is exempted from access pursuant to 5 U.S.C. 552a(j)(2) and/or (k)(2). A determination as to the applicability of the exemption to a particular record(s) shall be made at the time a request for access is received.

Contesting record procedures:

Same as above.

Record source categories:

Records are generated by: individuals covered by the system; Bureau staff; federal, state, local, tribal, international, and foreign law enforcement agencies; and federal/state probate and judicial offices.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(3), (e)(5), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and/or Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (e) and have been published in the *Federal Register*. The rules are published at 28 CFR 16.97(e) and (f).

[\[TOP\]](#)

JUSTICE/BOP-012

System name:

Office of Internal Affairs Investigative Records.

System location:

Records may be retained at the Central Office, Regional Offices, or at any of the Federal Bureau of Prisons (Bureau) or at any location operated by a contractor authorized to provide correctional, medical, and/or computer service to the Bureau. A list of Bureau system locations may be found at 28 CFR part 503 and on the Internet at <http://www.bop.gov>.

Categories of individuals covered by the system:

In connection with its investigative duties, the Office of Internal Affairs (OIA) maintains records on the following categories of individuals:

(a) Individuals or entities who are or have been the subject of investigations conducted by the Bureau including current or former employees of the Bureau; current and former consultants, contractors, and subcontractors with whom the agency has contracted and their employees.

grantees to whom the BOP has awarded grants and their employees; and such other individuals or entities whose association with the Bureau relates to alleged violation(s) of Bureau's rules of conduct, the Civil Service merit system, and/or criminal or civil law, which affect the integrity or physical facilities of the Bureau, including inmates and all visitors to Bureau facilities; and

(b) Individuals who are witnesses; complainants; confidential or nonconfidential informants and parties who have been identified by the Bureau or by other agencies, by constituents of the Bureau or by members of the general public as potential subjects of or parties to investigation under the jurisdiction of the Bureau, OIA.

Categories of records in the system:

OIA records fall into the following three categories:

1. "Information files" : Information received by OIA staff that is unrelated to current investigations and which does not suggest that administrative misconduct was probable allegations of staff actions that are performance related.
2. "Complaint files" : Database entries and hard copies of all allegations received, including those that are screened out and do not generally develop into OIA investigations because the matter may be too old, for example.
3. "Investigation files" , also known as "case files" : Information relating to OIA investigations including:
 - (a) Letters, memoranda, and other documents citing complaints of alleged criminal, civil administrative misconduct;
 - (b) Reports of investigations to resolve allegations of misconduct or violations of law with related exhibits, statements, affidavits or records obtained during investigations; prior criminal or noncriminal records of individuals as they relate to the investigations; reports from or law enforcement bodies; information obtained from informants; nature of allegations made against suspects and identifying data concerning such suspects; and public source material.

Authority for maintenance of the system:

Inspector General Act of 1978, 5 U.S.C. App. 3, as amended by the Inspector General / Amendments of 1988.

Purpose(s):

The Bureau, OIA maintains this system of records in order to conduct its responsibilities pursuant to the Inspector General Act of 1978, 5 U.S.C. App. 3, as amended by the Inspector General Act of 1988. The OIA is statutorily directed to conduct and supervise investigations relating to programs and operations of the Bureau; to promote economy, efficiency, and effectiveness in the administration of such programs and operations; and to prevent and fraud, waste and abuse in such programs and operations. Accordingly, the records in the system are used in the course of investigating individuals and entities suspected of having committed illegal and unethical acts in conducting related criminal prosecutions, civil proceedings, or administrative actions.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records in this system may be disclosed as follows:

(a) In the event that records indicate a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular provision of statute, or by rule, regulation, or order pursuant thereto, or if records indicate a violation or potential violation of the terms of a contract or grant, the relevant records may be disclosed to the appropriate agency, whether federal, state, local, foreign or international, charged with the responsibility of investigating or prosecuting such violation, enforcing or implementing such statute, rule, regulation or order, or with enforcing the terms of such contract or grant;

(b) A record may be disclosed to a federal, state, local, foreign or international agency, individual or organization when necessary to elicit information which will assist an investigation or audit;

(c) A record may be disclosed to a federal, state, local, foreign or international agency maintaining civil, criminal or other relevant information if necessary to obtain information relevant to a Bureau decision concerning the assignment, hiring or retention of an individual, the issuance or revocation of a security clearance, the reporting of an investigation of an

individual, the letting of a contract, or the issuance or revocation of a license, grant, or other benefit;

(d) A record may be disclosed to a federal, state, local, foreign or international agency, or a contract correctional company, in connection with the assignment, hiring or retention of an individual, the issuance or revocation of a license, grant, or other benefit by the agency to the extent that the information is relevant and necessary to the agency's decision on the matter;

(e) A record may be disclosed to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(f) Relevant records may be disclosed to an administrative forum, including ad hoc forums, which may or may not include an Administrative Law Judge, and which may or may not convene public hearings/proceedings, or to other established adjudicatory or regulatory agencies, e.g., the Merit Systems Protection Board, the National Labor Relations Board or other agencies with similar or related statutory responsibilities, where necessary to adjudicate decisions affecting individuals who are the subject of OIA investigations and/or who are covered by this system, including (but not limited to) decisions to effect any necessary remedial actions, e.g., the initiation of debt collection activity, disciplinary and/or other appropriate personnel action, and/or other law enforcement related actions, where appropriate;

(g) A record may be disclosed to complainants and/or victims to the extent necessary to provide such persons with information concerning the results of the investigation or case arising from the matters of which they complained and/or of which they were a victim;

(h) A record may be disclosed to the National Archives and Records Administration and General Services Administration during a records management inspection conducted under U.S.C. 2904 and 2906;

(i) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system's records; and

(j) Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose

relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored in electronic media in Bureau facilities via configuration of personal computer, client/server, and mainframe systems architecture. Computerized records are maintained on hard disk, Compact Discs (CDs), floppy diskette, magnetic tapes and/or optical disks. Documentary records are maintained in manual file folders, microfilm and/or index card files.

Retrievability:

Entries are arranged alphabetically and are retrieved with reference to the surname of the individuals covered by this system of records.

Safeguards:

Information is safeguarded in accordance with Bureau rules and policy governing sensitive data and automated information system security and access. These safeguards include maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Only those Bureau personnel who require access to perform their official duties may access the system equipment and the information in the system. Manual records are stored in safes and locked filing cabinets in secured rooms or in guarded buildings.

Retention and disposal:

Records in this system are retained as follows: (1) "Information files" are maintained for one year from the time the information is received; (2) "complaint files" are maintained for five

years from the date of the database entry; and (3) "investigation files" are retained for the (30) years from the year the OIA investigation is begun. Documentary records are destroyed by shredding; computer records are destroyed by degaussing and/or shredding.

System manager(s) and address:

Assistant Director/ General Counsel, Federal Bureau of Prisons, 320 First Street NW, Washington, DC 20534.

Notification procedure:

Inquiries concerning this system should be directed to the System Manager listed above.

Record access procedures:

The major part of this system is exempted from this requirement pursuant to 5 U.S.C. 552(j)(2), (k)(1), and (k)(2). To the extent that this system of records is not subject to exemption, it is subject to access. A determination as to exemption shall be made at the time a request for access is received. A request for access to records contained in this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Act Request." Include in the request the full name of the individual involved, his or her current address, date and place of birth, notarized signature, and any other identifying number or information which may be of assistance in locating the record. The requester shall also provide a return address for transmitting the information. Access requests shall be directed to the System Manager listed above.

Contesting record procedures:

Same as above.

Record source categories:

The subjects of investigations; individuals with whom the subjects of investigations are associated; current and former BOP officers and employees; officials of federal, state, local, and foreign law enforcement and non-law enforcement agencies; private citizens, witnesses, confidential and nonconfidential informants; and public source materials.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) (3), (5), and (8) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). In addition, the system has been exempted from subsections (c)(3), (d), and (e)(1) pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/BOP-013

System name:

Inmate Electronic Message Record System.

Security classification:

Not classified.

System location:

For the pilot program, records will be retained only at selected sites. Once the pilot is completed and evaluated, records may be retained at any of the Federal Bureau of Prisons (Bureau) facilities nationwide, or at any location operated by a contractor authorized to provide computer and/or electronic message service to Bureau inmates. A list of Bureau facilities may be found at 28 CFR part 503 and on the Internet at <http://www.bop.gov>.

Categories of individuals covered by the system:

Current and former inmates, including pre-trial detainees, under the custody of the Attorney General and/or the Director of the Bureau of Prisons; recipients of electronic messages from current and former inmates; individuals on the approved electronic message correspondent lists of current or former inmates; individuals who request, in writing through either traditional mail or through electronic message, that the Bureau delete their name and electronic address from inmate electronic message correspondent lists.

Categories of records in the system:

Records in this system include: (1) Personal identification data; (2) time usage data; (3) electronic message data, including date and time of each electronic message; the name and register number of the inmate who sent the electronic message; and the electronic address of the message recipient and his/her relationship to the inmate; digital and compact disc recordings of electronic messages; and (4) investigatory data developed internally as well as any related data collected from federal, state, local, tribal and foreign law enforcement agencies, and from federal and state probation and judicial officers.

Authority for maintenance of the system:

18 U.S.C. 3621, 4042, and 5003.

Purpose(s):

This system of records is maintained to manage records relating to inmate electronic messages and to ensure that inmates exercise their electronic message privileges in a manner consistent with correctional goals. The Bureau of Prisons encourages inmates to maintain contact with members of the community, including contact through the exchange of electronic messages directed to socially useful goals. The related uses for which the Bureau will maintain the system include (1) recording of time used by inmates writing, receiving, and reviewing electronic messages; (2) maintaining inmate electronic message correspondent lists; (3) monitoring of inmate electronic message activity; and (4) conducting investigations, e.g., investigation of inmate activity related to electronic message usage, and/or illegal activities suspected illegal activities being conducted, coordinated, or directed from within a federal correctional institution.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant data from this system will be disclosed as follows:

(a) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, tribal or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities, including possible criminal violations discovered as part of

electronic message monitoring done for the safety, security and good order of penal institutions.

(b) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;

(c) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the record subject;

(d) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(e) To the National Archives and Records Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(f) To affected non-inmate record subjects to the extent necessary to provide such persons information concerning placement and/or removal from an inmate's electronic message correspondent list;

(g) To an individual, organization, or governmental entity in order to notify them of a serious terrorist threat for the purpose of guarding against or responding to such a threat;

(h) In an appropriate proceeding before a court, or administrative or adjudicative body where the Department of Justice determines that the records are arguably relevant to the proceeding or in an appropriate proceeding before a court, or administrative or adjudicative body, where an adjudicator determines the records to be relevant to the proceeding;

(i) The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee where such communications may be necessary for personnel-related or other official purposes where the Department

requires information and/or consultation assistance from the former employee regarding matter within that person's former area of responsibility; and

(j) To federal, state, local, tribal, foreign or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license permit.

Disclosure to consumer reporting agencies:

Not Applicable.

Policies and practices for storing, retrieving, accessing, RETAINING AND DISPOSING records in the system:

Storage:

Information maintained in the system is stored in electronic media via a configuration of personal computer and client/server, and may be accessed by those with a need-to-know. Bureau and contractor facilities. Some information may be stored in other computerized e.g., hard disk, floppy diskettes, magnetic tape, digital recordings, Compact Discs (CDs) and/or optical disks. Documentary records are maintained in manual file folders and/or index card files.

Retrievability:

Records may be retrieved by identifying data including name and/or register number of and/or by name and/or electronic address of message recipient or individual on approved inmate electronic message correspondent list.

Safeguards:

Information is safeguarded in accordance with Bureau rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Only those Bureau personnel and authorized contractors who require access to perform their official duties may access the system equipment and the information in the system. Bureau inmates will only be able to

access their own sent and received electronic messages.

Retention and disposal:

Electronic messages are maintained ordinarily for six months from the date created, at which time they are overwritten with new data. Other records in this system may be incorporated into another system of records, e.g., JUSTICE/BOP-005, Inmate Central Records System. System-generated reports are retained for as long as they are needed. Computerized records are destroyed by degaussing; documentary records are destroyed by shredding.

System manager(s) and address:

Assistant Director, Administration Division, Federal Bureau of Prisons, 320 First Street, NE, Washington, DC 20534.

Notification procedure:

Inquiries should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made by writing to the Federal Bureau of Prisons, 320 First Street, NW., Washington, DC 20534. The envelope should be clearly marked "Freedom of Information/Privacy Act Request." The request should include a general description of the records sought, including the approximate dates covered by the record, the requester's name, current address, and date, and place of birth. Also, if the requester is an inmate who requests documents to be sent to a third party, the inmate must provide with the request an example of his or her signature, which must be verified and dated within three (3) months of the date of request. This system of records is exempted from access pursuant to 5 U.S.C. 552a(j)(2) and/or (k)(2). A determination as to the applicability of the exemption to a particular record(s) shall be made at the time a request for access is received.

Contesting record procedures:

Same as above. Requesters may contest record procedures by writing to the Office of Information and Privacy, U.S. Department of Justice, Federal Bureau of Prisons, 320 First Street, NW., Washington, DC 20530.

Record source categories:

Records are generated by: individuals covered by the system; Bureau staff; federal, state, local, tribal, international and foreign law enforcement agencies; and federal/state probate and judicial offices.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d)(1)-(e)(2), (e)(3), (e)(5), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and/or (k). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/BOP-014

System name:

Employee Assistance Program Record System.

System location:

Records may be retained at the Central Office, Regional Offices, and at any of the Bureau Prisons (Bureau) facilities. A list of these system locations may be found at 28 CFR part 201 and on the Internet at <http://www.bop.gov>.

Categories of individuals covered by the system:

Current and former employees of the Bureau of Prisons who have sought counseling or referred for treatment or referral through the Employee Assistance Program (EAP). To a limited degree that treatment and referral may be provided to family members of Bureau employees, these individuals are also covered by the system. The remainder of this notice refer to all persons covered by the system as "EAP client(s)."

Categories of records in the system:

The system contains records of EAP clients who have sought or been referred to the EAP treatment and/or referral. These records may include the following:

- (1) Identification data, including name, Social Security number, driver's license number, Bureau employee number, EAP system-generated number, job title and/or series, age and date of birth, sex, financial history, medical/mental health insurance information, home and work addresses, e-mail addresses and telephone numbers;
- (2) Information from other Bureau staff and/or the employee's supervisor, on work place performance problems, address and telephone numbers for the supervisor and/or other Bureau staff, and referral memoranda and/or e-mail correspondence from the employee supervisor and/or other staff;
- (3) Information and correspondence from outside sources, e.g. initial contacts from inter persons who are not Bureau staff;
- (4) Information generated by EAP staff concerning the EAP client, including background information, assessment, prognosis and counseling details;
- (5) Information concerning referrals to community-based treatment programs or individuals including the initial referral, addresses, telephone numbers, and credentials of treatment facilities or individuals providing treatment, and records of the employee's attendance, treatment accounts, and progress;
- (6) Pertinent employee records including leave and/or work Time and Attendance (T and Attendance) records, written consent forms, disciplinary actions and/or abeyance agreements, drug test records and information on confirmed unjustified positive drug tests.

Authority for maintenance of the system:

42 U.S.C. 290dd et seq.; 42 CFR part 2; Executive Order 12564; 5 U.S.C. 3301, 7361, 7901 and 7904; 44 U.S.C. 3101 and Pub. L. 100-71, 101 Stat. 391, Sec. 503 (July 11, 1988)

Purpose(s):

These records assist EAP staff in the execution of its assessment, counseling and referral

function. They document the nature and effects of EAP client problems and counseling EAP staff, referral to, and participation in, outside treatment and counseling programs, and EAP client's progress. These records may also be used to track compliance with abeyance agreements made to mitigate employee discipline actions.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant data from this system will be disclosed as follows:

- (a) To appropriate State or local authorities to report incidents of suspected child, elder, domestic abuse and/or neglect, as required under State law;
- (b) To any person or entity to the extent necessary to meet a bona fide medical emergency;
- (c) To any person or entity to the extent necessary to prevent immediate loss of life or serious bodily injury;
- (d) To referral community health care providers authorized to provide services to EAP clients to the extent that it is appropriate, relevant, and necessary to enable the provider to perform services as evaluation, counseling, treatment, and/or rehabilitation; and
- (e) To any person who is responsible for the care of an EAP client when the EAP client whom the records pertain is mentally incompetent or under legal disability.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Documentary records are maintained in manual file folders and/or index cards and stored in locked GSA security-approved containers. Computer records are stored in electronic media in a configuration of personal computer, client/server, and mainframe systems architecture including hard drives, floppy diskettes, CDs, magnetic tape, and/or optical disks.

Retrievability:

Records are indexed and retrieved only by a personal code number generated by the system.

Safeguards:

Electronic information is safeguarded in accordance with Bureau of Prisons rules and policies governing automated information systems security and access. These safeguards include maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Documentary records are kept in locked GSA security-approved containers in restricted access buildings. Only the EAP Administrator or designated Bureau staff will access or disclose the records.

Retention and disposal:

Records are retained for three years after the EAP client ceases contact with the EAP counselor (in accordance with General Records Schedule No. 1, Item No. 26) unless a longer retention period is necessary because of pending administrative or judicial proceedings. In such cases, the records are retained for six months after the case is closed. Computerized records are destroyed by shredding, degaussing, etc., and documentary records are destroyed by shredding. All destruction of records must be performed by an EAP staff member.

System manager(s) and address:

National Employee Assistance Program Coordinator, Federal Bureau of Prisons, 320 First Street NW., Washington, DC 20534.

Notification procedure:

Inquiries concerning this system should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made in writing to the Director, Federal Bureau of Prisons, First Street NW., Washington, DC 20534, and should be clearly marked "Privacy Act Request." In addition to a return address, requesters should provide the full name and notarized signature of the individual who is the subject of the record and is authorizing release of information, the dates during which the individual was in counseling, and any other information.

which may assist in identifying and locating the record. Pursuant to 28 CFR 16.41(d), an original signature on a "Certification of Identity" form (DOJ-361) may be submitted in lieu of a notarized signature. This form may be obtained from the Department of Justice website <http://www.usdoj.gov> or by writing to the FOIA/PA Office, Bureau of Prisons, 320 First Street, NE, Washington, DC 20534.

Contesting record procedures:

All requests to contest or amend information should be directed to the Director of the Federal Bureau of Prisons at the address listed above. The request should follow the Record Access Procedures, listed above, and should state clearly and concisely the information being contested, the reason for contesting it, and the proposed amendment thereof. The envelope should be clearly marked, "Privacy Act Request."

Record source categories:

Records are generated by Bureau staff, outside sources, referral counseling and treatment programs or individuals, and the EAP client who is the subject of the record. In the case of drug abuse counseling, records also may be generated by staff of the Drug-Free Workplace Program and the Medical Review Officer.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/BOP-015

System name:

Outside Employment Requests Record System.

System location:

Records may be retained at the Central Office, Regional Offices, and/or at any of the Federal Bureau of Prisons (Bureau) facilities. A list of these system locations may be found at 28

part 503 and on the Internet at <http://www.bop.gov>.

Categories of individuals covered by the system:

Current and former Bureau employees, including the following professionals: attorneys, doctors, psychiatrists, chaplains and architects, who request approval for outside employment.

Categories of records in the system:

Submitted requests for permission to be employed outside the Bureau; staff notes, correspondence and/or memoranda concerning the processing of these requests; approved/disapproved requests signed by appropriate Bureau officials; identifying data intended employers, including name, address, telephone number, point of contact; identifying data of Bureau employee, including name, duty location, address, telephone number, and a system-generated number.

Authority for maintenance of the system:

This system is established and maintained under the authority of 5 CFR 3801.106.

Purpose(s):

The purpose of this system is to track approved and disapproved requests by Bureau employees for outside employment, including the following professions: attorneys, doctors, psychiatrists, chaplains and architects.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

In addition to Bureau employees who have a need for the information in the course of their duties, relevant data from this system will be disclosed as follows:

(a) To federal, state, local, tribal, foreign and international law enforcement agencies and officials for law enforcement purposes such as investigations, possible criminal prosecutions, civil court actions, and/or regulatory proceedings;

(b) To a court or adjudicative body before which the Department of Justice or the Bureau

authorized to appear when any of the following is a party to litigation or has an interest in litigation and such records are determined by the Bureau to be arguably relevant to the litigation; (1) the Bureau, or any subdivision thereof, or (2) any Department or Bureau employee in his or her official capacity, or (3) any Department or Bureau employee in his or her individual capacity where the Department has agreed to provide representation for the employee, or (4) the United States, where the Bureau determines that the litigation is likely to affect it or any of its subdivisions;

(c) In an appropriate proceeding before a court or administrative or regulatory body where records are determined by the Department of Justice to be arguably relevant to the proceeding, including federal, state, and local licensing agencies or associations which disseminate information concerning the suitability or eligibility of an individual for a license or permit;

(d) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record;

(e) To the National Archives and Records Administration and General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(f) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system's records; and

(g) Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Information maintained in the system is stored in electronic media in Bureau facilities via configuration of personal computer, client/server, and mainframe systems architecture. Computerized records are maintained on hard disk, floppy diskettes, compact discs (CD), magnetic tapes and/or optical disks. Documentary records are maintained in manual file and/or index card files.

Retrievability:

Documentary records are sorted by year, and then filed alphabetically by the subject's last name. Computerized data is retrievable by the fields entered into the data-base, including name, duty location, date, region, and the system-generated number.

Safeguards:

Information is safeguarded in accordance with Bureau rules and policy governing automatic information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Only those Bureau personnel who require access to perform their official duties may access the system equipment and the information in the system.

Retention and disposal:

Records are reviewed every two years and are retained for seven (7) years from the date of approval/disapproval of the request. Documentary records are destroyed by shredding; electronic records are destroyed by either erasing or degaussing.

System manager(s) and address:

Assistant Directory/General Counsel, Office of General Counsel, Federal Bureau of Prisons
320 First Street NW, Washington, DC 20534.

Notification procedure:

Inquiries concerning this system should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made in writing to the Director, Federal Bureau of Prisons, First Street NW, Washington, DC 20534, and should be clearly marked "Privacy Act Request".

Contesting record procedures:

Same as above.

Record source categories:

Records are generated by Bureau employees who submit requests for permission to be employed outside the Bureau, by Bureau staff involved in the processing of these requests, and by intended employers.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/BOP-101

System name:

National Institute of Corrections Technical Resource Provider Record System.

System location:

Records may be retained at the National Institute of Corrections (NIC) headquarters in Washington, DC or in NIC field Offices, e.g., the NIC Academy campus currently located in Longmont, Colorado.

Categories of individuals covered by the system:

Individuals who have been identified and have agreed to provide technical and/or training assistance to state, local, tribal, foreign and international correctional agencies in order

strengthen and improve the practice of corrections. These individuals are referred to as Technical Resource Providers (TRPs).

Categories of records in the system:

Records in this system include: (1) Identification and/or logistical information for each TRP including name, mailing address and telephone numbers; (2) resume and/or biographic information of each TRP, including educational and work experience; (3) program information concerning the subject area of expertise and descriptive comments provided by each TRP; (4) records generated by the system listing TRPs i.e. database printouts which include information enumerated in (1), (2), and (3) above.

Authority for maintenance of the system:

This system is established and maintained under the authority of 18 U.S.C. 4352.

Purpose(s):

Recent technological developments are making it possible for the National Institute of Corrections (NIC) to consolidate and automate its directory of individuals available to provide technical and/or training assistance to corrections agencies. These individuals are currently called Technical Resource Providers (TRPs) and the information about each TRP that is contained in this system assists NIC in identifying appropriate TRPs to staff corrections seminars and provide technical assistance.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant data from this system will be disclosed as follows:

- (a) To federal agencies, and/or state, local, tribal, foreign and international government agencies that have a need for the information in the performance of their official duties.
- (b) To individuals, groups or private correction companies who request technical assistance and/or training in corrections.
- (c) To officials and/or contractors of federal, state, local, tribal, foreign and international

enforcement agencies for law enforcement purposes such as investigations, possible or prosecutions, civil court actions, and/or regulatory proceedings.

(d) To employees and/or contractors of the National Archives and Records Administration General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations facilitating communications with a former employee that may be necessary for personnel related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored in hard copy and/or electronic media in National facilities via a configuration of personal computer, client/server, and mainframe systems architecture. Computerized records are maintained on hard disk, floppy diskettes, magnetic tapes and/or optical disks. Documentary records are maintained in manual file folders and index cards.

Retrievability:

Records are retrievable by identification/logistical information, e.g. name and address of individual and/or by the subject area of expertise.

Safeguard:

Information is safeguarded in accordance with Department of Justice and Bureau of Prisons rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas.

locked offices and locked file cabinets in controlled-access buildings, and the required proper passwords and user identification codes to access the system. Only those NIC personnel who require access to perform their official duties may access the system equipment and the information in the system.

Retention and disposal:

Electronic records generated by the system are retained until such time as the records no longer serve the purpose described by this system. At such time, these records may be updated and/or incorporated into an appropriate, published system or records with an approved retention schedule, or otherwise destroyed by shredding and/or degaussing. Documentary records are retained for eight (8) years and then destroyed by shredding.

System manager(s) and address:

Director, National Institute of Corrections, Room 5007, 320 First St. NW, Washington, D 20534.

Notification procedure:

Inquiries concerning this system should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made in writing to the Director, National Institute of Corrections, Room 5007, 320 First St. NW, Washington, DC 20534, and should be clearly marked "FOIA Request."

Contesting record procedures:

Same as above.

Record source categories:

Records are generated by individuals listed as a TRP, by NIC staff, and/or staff from other correctional and/or other law enforcement agencies.

Systems exempted from certain provisions of the Act:

None.

[\[TOP\]](#)

JUSTICE/BOP-102

System name:

National Institute of Corrections Field Readers List.

System location:

Records will be retained at the National Institute of Corrections (NIC), 320 First Street, N
Washington, DC 20534.

Categories of individuals covered by the system:

Persons with expertise in a field of corrections who have been approved by the Advisory
of NIC and who have agreed to review applications for grants where the amount of the grant
exceeds 100,000 dollars or where a substantial personal conflict of interest is indicated.

Categories of records in the system:

(1) Resume of individual including educational and work experience information; and (2)
expertise checklist completed by the individual.

Authority for maintenance of the system:

This system is established and maintained under the authority of 18 U.S.C. 4352(a).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The routine uses of this system are: (a) To provide an information source to officers and
employees of the Department of Justice who have a need for the information in the

performance of their duties; and (b) to provide the Advisory Board of NIC with a list of individuals who have the expertise to review applications for grants where the amount of award exceeds 100,000 dollars or where a substantial personal conflict of interest is indicated.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system may be stored on documents, magnetic tape, and magnetic disk.

Retrievability:

Information is indexed by name and areas of expertise.

Safeguards:

Information is safeguarded in accordance with Bureau of Prisons rules governing access and release.

Retention and disposal:

All records will be maintained until either the individual notifies NIC that he or she no longer desires to provide assistance or until the Advisory Board of NIC determines that a name should be deleted from the list. If deleted for any reason, the records will be destroyed by shredding.

System manager(s) and address:

Administrative Officer, National Institute of Corrections, 320 First Street, NW, Room 200

Washington, DC 20534.

Notification procedure:

Address inquiries to: Director, National Institute of Corrections, 320 First Street, NW, Room 200, Washington, DC 20534.

Record access procedures:

Same as notification procedure.

Contesting record procedures:

Same as notification procedure.

Record source categories:

All information is obtained from the individual named in the list.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/BOP-103

System name:

National Institute of Corrections Academy Record System.

System location:

Records may be retained at the national headquarters of the National Institute of Corrections (NIC) and/or at the NIC Academy campus currently located in Longmont, Colorado.

Categories of individuals covered by the system:

NIC staff; training instructors also known as Technical Research Providers (TRP) contra the NIC Academy; corrections staff student applicants from federal, state, local, tribal, foreign and international government agencies, including corrections and other law enforcement agencies; employees from private corrections companies who have contracted to provide corrections services to government agencies.

Categories of records in the system:

Records in this system include: (1) Identification and logistical information for applicants, students, and TRPs at NIC Academy seminars, including name, gender, race, address, telephone number, Social Security number, position title, training history, professional history; (2) seminar applications; (3) seminar information including dates and location of each seminar and name of seminar coordinator; (4) financial/procurement data for each seminar, including budget information, printing orders and travel costs for TRPs and participants.

Authority for maintenance of the system:

This system is established and maintained under the authority of 18 U.S.C. 4352.

Purpose(s):

The purpose of this system is to maintain a current database of student applicants, participants and instructors, or Technical Research Providers (TRPs) at NIC Academy training seminars; track all expenditures related to each training seminar; and to maintain current biographical data on NIC staff and TRPs.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant data from this system will be disclosed as follows:

(a) To contractors or employees of the Department of Justice and/or other federal agency and/or state, local, tribal, foreign and international government agencies or professional organizations who have a need for the information in the performance of their official duties, e.g., when the employees are participating in NIC seminars or when the agencies seek information for their own purposes, such as training, budgeting, staffing, etc.;

(b) To federal, state, local, tribal, foreign and international law enforcement agencies and officials for law enforcement purposes such as investigations, possible criminal prosecution, civil court actions, and/or regulatory proceedings;

(c) To a court or adjudicative body before which the Department of Justice or the Bureau is authorized to appear when any of the following is a party to litigation or has an interest in litigation and such records are determined by NIC to be arguably relevant to the litigation: (1) any NIC, the Bureau, or any subdivision thereof, or (2) any NIC, Bureau, or Department of Justice employee in his or her official capacity, or (3) any NIC, Bureau, or Department of Justice employee in his or her individual capacity where the Department of Justice has agreed to provide representation for the employee, or (4) the United States, where NIC or the Bureau determines that the litigation is likely to affect it or any of its subdivisions;

(d) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record;

(e) To the National Archives and Records Administration and General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations, facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored in electronic media in NIC Academy and/

headquarters offices via a configuration of personal computer, client/server, and mainframe systems architecture. Computerized records are maintained on hard disk, floppy diskette, magnetic tapes and/or optical disks. Documentary records are maintained in manual file and/or index cards.

Retrievability:

Records are retrievable by identification information, e.g., names, locations of TRP staff, student applicants; seminar information, e.g., subject, date and place of the seminar.

Safeguards:

Information is safeguarded in accordance with Bureau of Prisons rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the system. Only those NIC personnel who require access to perform their official duties may access the system equipment and the information in the system.

Retention and disposal:

Biographical information about NIC staff and Technical Resource Providers (TRPs) is maintained for three (3) years and then either updated or destroyed by shredding and/or degaussing. Information about student applicants is maintained until such time as they no longer serve the purpose described by this system. At such time, these records may be incorporated into an appropriate, published system of records with an approved retention schedule, or otherwise destroyed by shredding and/or degaussing.

System manager(s) and address:

Director, National Institute of Corrections, Room 5007, 320 First Street NW, Washington, DC 20534.

Notification procedure:

Inquiries concerning this system should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made in writing to the Director, National Institute of Corrections, Room 5007, 320 First Street NW, Washington, DC 20534, and should be clearly marked "Privacy Act Request."

Contesting record procedures:

Same as above.

Record source categories:

Records are generated by NIC staff and by individuals desiring to attend NIC seminars.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/BOP-104

System name:

National Institute of Corrections Mailing List and Information Center Contacts Record System

System location:

Records may be retained at the national headquarters of the National Institute of Corrections (NIC) and/or at the NIC Information Center currently located in Longmont, Colorado and the offices of an information management company authorized by contract with NIC to receive and manage the system.

Categories of individuals covered by the system:

Individuals who request corrections information from the NIC Information Center and
Individuals who receive NIC-generated mailings of corrections information, including (1)

constituents sorted by constituent group, e.g. directors or commissioners of state Departments of Corrections, administrators of large jails, NIC Advisory Board members; (2) employees of federal, state, local, tribal, foreign and international government agencies, including courts and other law enforcement agencies; (3) employees from private corrections companies who have contracted to provide corrections services to government agencies; (4) inmates and inmate family members and friends; (5) elected officials including Members of Congress; members of professional organizations including the American Corrections Association; members of the news media; (8) members of the general public, including staff and students from educational institutions and charitable organizations.

Categories of records in the system:

Records in this system include: (1) Identification and logistical information for persons who contact the Information Center, e.g. name, agency, address, telephone number; library codes of documents requested and sent, receipt and response dates, method of information delivery, postage costs; (2) Names and addresses of NIC constituents, sorted by constituent group, e.g. directors or commissioners of state Departments of Corrections, administrators of large jails, NIC Advisory Board members.

Authority for maintenance of the system:

This system is established and maintained under the authority of 18 U.S.C. 4352.

Purpose(s):

The purpose of this system is to more efficiently track and respond to persons who request information from the NIC Information Center and to generate labels for NIC-initiated mail groups of NIC constituents.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant data from this system will be disclosed as follows:

(a) To contractors or employees of the Department of Justice and/or other federal agencies and/or state, local, tribal, foreign and international government agencies or professional organizations who have a need for the information in the performance of their official duties.

e.g. when the employees will use the mailing list to initiate mailings approved by NIC.

(b) To the National Archives and Records Administration and General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations facilitating communications with a former employee that may be necessary for personnel related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored in electronic media via a configuration of personal computer, client/server, and mainframe systems architecture located in the NIC Information Center and/or NIC headquarters offices and/or the offices of an information management company authorized by contract with NIC to maintain and manage the system. Computerized records are maintained on hard disk, floppy diskettes, magnetic tapes and optical disks. Documentary records are maintained in manual file folders and/or index cards.

Retrievability:

Records concerning persons who request information from the NIC Information Center are retrievable by identification and logistical information, e.g., name, address. Records concerning groups of NIC constituents who receive NIC-generated mailings are retrievable by category, constituent group, e.g. sheriffs; by position in the constituent group, e.g. sheriff of Fairfax County; and/or by certain identification information (names, addresses) of the individual constituent group, e.g. Sheriff John Smith.

Safeguards:

Information is safeguarded in accordance with Department of Justice and Bureau of Prisons rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas and the required use of proper passwords and user identification codes to access the system. Only those NIC personnel or authorized contractor staff who require access to perform their official and/or contract duties may access the system equipment and the information in the system.

Retention and disposal:

Information is maintained until such time as the records no longer serve the purpose defined by this system. At such time, these records may be updated or incorporated into an appropriate, published system of records with an approved retention schedule, or otherwise destroyed by shredding and/or degaussing.

System manager(s) and address:

Director, National Institute of Corrections, Room 5007, 320 First Street NW, Washington, DC 20534.

Notification procedure:

Inquiries concerning this system should be directed to the System Manager listed above.

Record access procedures:

All requests for records may be made in writing to the Director, National Institute of Corrections, Room 5007, 320 First Street NW, Washington, DC 20534, and should be clearly marked "Privacy Act Request."

Contesting record procedures:

Same as above.

Record source categories:

Records are generated by NIC staff and/or by persons requesting information from the

Information Center and/or by NIC constituents seeking NIC-generated mailings.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

Civil Division

JUSTICE/CIV-001

System name:

Civil Division Case File System.

System location:

Civil Division, U.S. Department of Justice 10th Street NW, Washington, DC 20530; Records Management Unit, 5320 Marinelli Road, Rockville, MD 20652; and Federal Records Center, Suitland, MD 20409.

Categories of individuals covered by the system:

Individuals referenced in potential or actual cases and matters under the jurisdiction of the Civil Division; and attorneys, paralegal, and other employees of the Civil Division directly involved in these cases or matters.

Categories of records in the system:

(1) Records in this system pertain to a broad variety of litigation under the jurisdiction of the Civil Division relating to torts, civil fraud and other commercial matters, federal programs, national security, immigration, and consumer issues. The case files contain court records, agency and intra-agency correspondence, and legal research. These records may include investigatory and/or criminal law enforcement information and information classified pursuant to Executive Order to protect national security interests. (2) Summary information (i.e., names of principal parties or subjects, case file numbers, assignments, status, and classification) for these cases or matters is maintained prior to FY 78 on index cards and from FY 78 in an

automated case tracking system. (3) A timekeeping function for attorneys, paralegal, and employees of the Civil Division directly involved in litigation supplements the automated tracking system from May of 1981.

Authority for maintenance of the system:

General authority to maintain the system is contained in 5 U.S.C. 301 and 44 U.S.C. 31. A particular system was established in accordance with 28 CFR 0.77(f) and 28 U.S.C. 552 was delegated to the Civil Division pursuant to the memorandum from the Deputy Attorney General, dated July 17, 1974.

Purpose(s):

Case records are maintained for the purpose of litigating or resolving any case or matter under consideration by the Civil Division. The automated case tracking and timekeeping system is maintained for the purpose of managing and evaluating the Division's litigative activities.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of a record as follows: (1) In any case in which there is an indication of a violation or potential violation of law, whether civil, criminal or regulatory in nature, the record in question may be disseminated to the appropriate federal, state, local or foreign agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law; (2) in the course of investigating the potential or actual violation of law, whether civil, criminal or regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing for such violation, a record may be disseminated to the federal, state, local or foreign agency, or to an individual or organization, if there is reasonable belief that such agency, individual or organization possesses information or is responsible for acquiring information relating to the investigation, trial or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or informant; (3) a record relating to a case or matter that has been referred by an agency for investigation, prosecution, or enforcement, or that involves a case or matter within the jurisdiction of an agency, or where the agency or officials thereof are a party to litigation where the agency or officials may be affected by a case or matter, may be disseminated to such agency to notify the agency of the status of the case or matter or of any decision concerning the case or matter.

determination that has been made, or to make such other inquiries and reports as are necessary during the processing of the case or matter; (4) a record relating to a case or may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States or to an executive agreement; (5) a record be disseminated to a federal, state, local, foreign, or international law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to investigative leads to such agency; (6) a record may be disseminated to a foreign country through the United States Department of State or directly to the representative of such country to the extent necessary to assist such country in civil or criminal proceedings in which the United States or one of its officers or agencies has an interest; (7) a record, or any facts derived therefrom, may be disclosed in a grand jury proceeding or in a proceeding before a court or adjudicative body before which the Civil Division is authorized to appear when the United States, or any agency or subdivision thereof, is a party to litigation and such record is determined by the Civil Division to be arguably relevant to the litigation; (8) to facilitate processing Freedom of Information and Privacy Act requests for these records, information may be disclosed to another Federal agency to (a) permit a decision as to access, amendment or correction of records to be made in consultation with or by that agency, or (b) verify the identity of an individual or the accuracy of information submitted by an individual who has requested access to or amendment or correction of records; (9) information may be released to the media and the public in accordance with 28 CFR 50.2 unless it is determined that release would constitute an unwarranted invasion of personal privacy; (10) a record may be disclosed to the National Archives and Records Administration and the General Services Administration for records management inspections conducted under the authority of 44 U.S.C. 2904 and (11) in any health care-related civil or criminal case, investigation, or matter, information indicating patient harm, neglect, or abuse, or poor or inadequate quality of care, at a health care facility or by a health care provider, may be disclosed as a routine use to any federal, state, local, tribal, foreign, joint, international or private entity that is responsible for regulating, licensing, registering, or accrediting any health care provider or health care facility, or enforcing any health care-related laws or regulations. Further, information indicating an ongoing quality of care problem by a health care provider or at a health care facility may be disclosed to an appropriate health plan. Additionally, unless otherwise prohibited by applicable law, information indicating patient harm, neglect, abuse, or poor or inadequate quality of care may be disclosed to the affected patient or his or her representative or guardian at the discretion and in the manner determined by the agency in possession of the information; (12) pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing

authority, in accordance with applicable Department regulations; or facilitating communication with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility; (13) information relating to health care fraud may be disclosed to private health plans, or associations of health plans, and health insurers, or associations of health insurers, for the following purposes: To promote the coordination of efforts to prevent, detect, investigate, and prosecute health care fraud; to assist efforts by victims of health care fraud to obtain restitution; to encourage private health plans to participate in local, regional, and national health care fraud task force activities; and to assist tribunals having jurisdiction over claims against private health plans; (14) for all claims made by individuals covered by the Energy Employees Occupational Compensation Program Act, Pub. L. 106-398, 114 Stat. 1654, Title XXXVI (2000), 42 U.S.C. 7384 et seq., the Civil Division may disclose to the Department of Labor all information contained in its Radiation Exposure Compensation Act, (42 U.S.C. 2210 note) files pertaining to those claims; (15) to contractors, experts, consultants employed by the Civil Division when necessary to accomplish an agency function related to this system of records.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Manual records are stored in file cabinets and on index cards. Automated records are stored on magnetic disks. Classified information is stored in locked safes.

Retrievability:

Manual records are retrieved by file number. This number can be obtained from index cards arranged alphabetically by subject name for records received prior to FY 78 and from local queries to the computer-based data for FY 78 and subsequent years.

Safeguards:

Classified information is maintained in locked safes. Access to all information is limited to Department of Justice personnel who have need for the records to perform their duties. Automated records are safeguarded and protected in accordance with Department rules and procedures governing the handling of computerized information.

Retention and disposal:

When a case file is closed by the responsible attorney, it is sent to the Federal Records for retention in accordance with the authorized Record Disposal Schedule for the classification of the case. Such schedules are approved by the National Archives.

After the designated period has passed, the file is destroyed. However, the index and document cards are not purged. Automated records constitute a cumulative resource file for which there are no plans to delete records.

System manager(s) and address:

Assistant Attorney General; Civil Division: U.S. Department of Justice; 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Address inquiries to: Assistant Attorney General; Civil Division; U.S. Department of Justice; 10th and Constitution Avenue, NW, Washington, DC 20530.

Record access procedures:

Portions of this system are exempt from disclosure and contest by 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). Submit in writing all requests for access to those portions not so exempted to the system manager identified above. Clearly mark the envelope and letter "FOI/PA Request" and provide a return address. The subject of the record should also provide his/her full name, notarized signature, date and place of birth, case caption, or other information which may assist in locating the records sought.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the Assistant Attorney General, Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530. The request should clearly state what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Information may be obtained from all individuals referred to in all cases or matters under consideration of the Civil Division. Timekeeping information is obtained from all Civil Division attorneys, paralegals, and other employees directly involved in such litigation or matters.

System exempted from certain provisions of the act:

The Attorney General has exempted certain categories of records in this system from subsections (c)(3) and (4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G) and (H), (e)(5), (e)(8), and the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1) and (k)(2). That is, these exemptions apply only to the extent that the file contains information which has been properly classified pursuant to an Executive Order, or to the extent that it contains investigatory and other law enforcement materials. Rules have been promulgated in accordance with the requirements of U.S.C. 552(b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/CIV-002

System name:

Civil Division Case File System: Customs Litigation.

System location:

26 Federal Plaza, New York, New York 10007, and U.S. Department of Justice Data Service Center, 10th and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

Any and all parties and counsel involved in the cases handled by the Field Office, Customs Litigation, Commercial Litigation Branch of the Civil Division will have identifying data contained in this system.

Categories of records in the system:

1. The main record of the system is the case file which is retained on each case under the jurisdiction of the Field Office, Customs Litigation, Commercial Litigation Branch of the Civil Division and constitutes the official record of the Department of Justice thereon. All record material relating to a case is retained in the file. Each file is assigned the Customs Court number given to the summons filed in that court or, in cases filed prior to October 1, 1970, the number assigned to reappraisement appeals or to protests filed with the Customs Court.

The number assigned to the file will change to the number assigned by the Court of Customs and Patent Appeals, if that case becomes the subject of an appeal before that court. In addition, the Custom Section retains a log of communications received and communications sent. The correspondence is identified thereon by court (case) number, identification of kind of communication, and the person receiving it.

2. The case file and communication logs are physically retained at the offices of the Field Office, Customs Litigation, Commercial Litigation Branch 26 Federal Plaza, New York, New York 10007. From these records, the Field Office, Customs Litigation, Commercial Litigation Branch inputs certain information for conversion into a data processing system which is maintained at the Department of Justice Data Services Center, 10th and Constitution Avenue NW, Washington, DC 20530. Included in the information contained in the data processing system is the identity of the parties and their counsel, as well as the merchandise involved, port of entry and the competing statutory provisions.

3. Alphabetical and numerical indices are maintained as a means of access to the proper number by the cross-referencing of the names of non-government parties to suit with the appropriate file (court) numbers. These indices are made of index cards and maintained in the Chief Clerk's office in the Field Office, Customs Litigation, Commercial Litigation Branch.

Authority for maintenance of the system:

The Field Office, Customs Litigation, Commercial Litigation Branch case files are maintained under the authority of 28 U.S.C. 2601(b) and 2632(e) and established in accordance with 28 CFR 0.45(c) which gives the Civil Division responsibility for 'all litigation incident to the reappraisement and classification of imported goods, including the defense of all suits in the Court of Customs and Patent Appeals', and with 28 CFR 0.48 which designates the Attorney-in-Charge, Field Office, Customs Litigation 'to accept service of notices of appeals to the Court of Customs and Patent Appeals and all pleadings and other papers filed in the Custom

when the United States is an adverse Party in any customs litigation'.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Any record pertaining to any case or matter in the Civil Division may be disseminated to other component of the Department of Justice, including the Federal Bureau of Investigation and the United States Attorney offices, for use in connection with the consideration of the case or matter or any other case or matter under consideration by the Civil Division or any other component of the Department of Justice.

Certain information contained in the record may also be disseminated to the U.S. Customs Service, the Department of the Treasury, the International Trade Commission, the Department of State, or any other agency of the Government whose decision is being challenged in a case assigned to the Field Office, Customs Litigation, Commercial Litigation Branch for disposition. Any record maintained in this system of records may be disseminated as a routine use of such record as follows: (1) In any case in which there is an indication of a violation or potential violation of law, whether civil, criminal or regulatory in nature, the record in question may be disseminated to the appropriate Federal, state, local or foreign agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law; (2) in the course of investigating the potential or actual violation of law, whether civil, criminal or regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing for such violation, a record may be disseminated to the appropriate Federal, state, local or foreign agency, or to an individual or organization, if there is reason to believe that such agency, individual or organization possesses information relating to the investigation, trial or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant; (3) a record relating to a case or matter may be disseminated in an appropriate Federal, state, local or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practice; (4) a record relating to a case or matter may be disseminated to a Federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing; (5) a record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion of such matters as settlement of the case or matter, plea bargaining, or formal or informal discovery proceedings; (6) a record relating to a case or matter that has been referred by an agency for investigation, prosecution, or enforcement; or that involves a case or matter within the jurisdiction of an agency, or where the agency or officials thereof are a party to the case or matter.

litigation or where the agency or officials may be affected by a case or matter, may be disseminated to such agency to notify the agency of the status of the case or matter or decision or determination that has been made, or to make such other inquiries and reports are necessary during the processing of the case or matter; (7) a record relating to a person held in custody pending or during arraignment, trial, sentence or extradition proceeding after conviction or after extradition proceedings, may be disseminated to a Federal, state or foreign prison, probation, parole, or pardon authority, or to any other agency or individual concerned with the maintenance, transportation, or release of such a person; (8) a record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States or to an executive agreement; (9) a record may be disseminated to a Federal, state, local, foreign or international law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency; (10) a record may be disseminated to a Federal agency, in response to its request, in connection with hiring or retention of an employee, the issuance of a security clearance, the reporting of investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter; (11) a record may be disseminated to the press, news media, trade associations, or organized groups, when the purpose of the dissemination is educational or informational, provided that the record does not contain any information identifiable to a specific individual other than is necessary to identify the matter or where the information has previously been filed in a judicial or administrative office, including the clerk of the court; (12) a record may be disseminated to a foreign country, through the United States Department of State or directly to the representative of such country, to the extent necessary to assist such country in civil or criminal proceedings in which the United States or one of its officers or agencies has an interest; (13) a record that contains classified national security information and material may be disseminated to persons who are engaged in historical research projects, or who have previously occupied policy making positions to which they were appointed by the President, in accordance with the provisions 28 CFR 17.60; (14) copies of documents, summons (protest and reappraisal appeals, where appropriate) and the communication logs are made available to employees of the private contractor who services the data processing system in New York for the purpose of enabling such employees to extract and transcribe pertinent information from said documents so that such information may be encoded and converted to punch card form.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of

maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 5 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

(1) The case files utilize standard file jackets or envelopes and are maintained in standard file cabinets; (2) The alphabetical index cards are maintained in standard file cabinets; (3) The communication logs are maintained in looseleaf binders and, when not being currently used, are also maintained in standard file cabinets; (4) The information in the data processing system is maintained on tapes stored in the Data Services Center.

Retrievability:

(1) The case files must be retrieved by number. The file number may be ascertained from

alphabetical index when the name of any non-government litigant is known. (2) The info contained in the data processing system may be retrieved through the retrieval tool acti by an attorney making a request for a report to the computer technician who codes the on a form in the format of the retrieval language. The action words of the retrieval report List-lists the case numbers of the cases which satisfy certain criteria such as plaintiff's r counsel's name, court, number, merchandise, competing statutory provisions, Governm counsel. Write—output and the full history for any case specified by case number. Write limited case history for any case specified by case number. Count-tallying the number c in the data base contained in the request.

Safeguards:

(1) Information contained in the system is unclassified. However, only attorneys in the C Division who have responsibility for the case may properly obtain a case file. Correspond and telephone calls about particular cases are referred to the attorney having responsib the case. In the attorney's absence, another attorney covering for the absent attorney o Attorney-in-Charge, Field Office, Customs Litigation may respond to the telephone call r correspondence. The index files and the communication logs are utilized only by the pe of the Field Office, Customs Litigation, Commercial Litigation Branch in locating or verify information contained in the system. (2) Information from the data processing system m obtained only by attorneys on the basis of requests made in writing on a proper form su by the Field Office, Customs Litigation, Commercial Litigation Branch. The request is m the computer technician. Normally these requests are mailed to the technician in charge Data Services Center, but occasionally the request may be related telephonically by the computer technician.

Retention and disposal:

(1) Closed case files are sent to the Federal Records Center for retention in accordance the authorized Records Disposal Schedule for the classification of the case. Such sched are approved by the National Archives. After the designated period is passed, the file is destroyed. The communication logs are sent to the Federal Records Center for retention accordance with the authorized records disposal schedule after five years. After the des period those records are also destroyed. The index cards, however, are not purged. (2) Periodically, the inactive cases will be purged from the main tape in the data processing system and transferred to the historical tape where the information will be retained inde There is a provision in the data processing system to delete and remove an entire case

from the main or historical tape. This may be done on request from the Attorney-in-Chief Field Office, Customs Litigation and such removed cases will not be saved or written on other tape.

System manager(s) and address:

Assistant Attorney General, Civil Division, U.S. Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Address inquiries to Assistant Attorney General, Civil Division, U.S. Department of Justice and Constitution Avenue, NW, Washington, DC 20530.

Record access procedures:

A request for information concerning the cases of the Field Office, Customs Litigation, Commercial Litigation Branch of the Civil Division should be submitted in writing, with the envelope and letter clearly marked "Privacy Access Request". The request should include file number and/or the names of any non-government litigant known to the requestor. The requestor should also provide a return address for transmitting the information. Such a request should be submitted to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the Assistant Attorney General, Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530. The request should clearly state what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

All litigants involved in the cases of this Division are sources of information. Such information is either contained in the record material in the case files or has been extracted from that material and put on communication logs and/or index cards.

[\[TOP\]](#)**JUSTICE/CIV-003**

System name:

Office of Alien Property File System.

System location:

550 11th Street, NW, Washington, DC 20530.

Categories of individuals covered by the system:

Any and all parties involved in the cases, claims and matters handled by the Office of Alien Property may have identifying data contained in this system.

Categories of records in the system:

1. This system consists of indices and files relative to enemy-owned property, reporting sources, ownership, vesting, and claims for the return thereof. Each vesting order is assigned a general file number, and each claim has a separate file number. Separate account files are maintained on vested property for each alien account.
2. Alphabetical and numerical indices are utilized as a means of access to the proper general file by the cross-referencing of the names of all individual former property owners and claimants with the general files.
3. Records of litigation involving the Office of Alien Property are contained in this system and are also alphabetical and numerical indices to facilitate access to these cases.

Authority for maintenance of the system:

The Office of Alien Property files are maintained under the authority of 44 U.S.C. 3101 and 44 U.S.C. App. 40, Title II of the International Claims Settlement Act, and was established in accordance with 28 CFR 0.47 which states in part `The Office of Alien Property shall be a part of the Civil Division ...` and thereafter describes the authority, rights, privileges, powers,

and functions of that office.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Any record pertaining to any case or matter in the Civil Division may be disseminated to other component of the Department of Justice, including the Federal Bureau of Investigation and the United States Attorney offices, for use in connection with the consideration of the case or matter or any other case or matter under consideration by the Civil Division or any other component of the Department of Justice.

Certain information contained in the record may also be disseminated to the U.S. Customs Service, the Department of the Treasury, the International Trade Commission, the Department of State, or any other agency of the Government whose decision is being challenged in a proceeding assigned to the Customs Section for disposition. A record maintained in this system of records may be disseminated as a routine use of such record as follows: (1) In any case in which there is an indication of a violation or potential violation of law, whether civil, criminal or regulatory in nature, the record in question may be disseminated to the appropriate Federal, state, local or foreign agency charged with the responsibility for investigating or prosecuting such violation, or to an agency charged with enforcing or implementing such law; (2) in the course of investigating the potential or actual violation of any law, whether civil, criminal or regulatory in nature, or in the course of a trial or hearing, or the preparation for a trial or hearing for such violation, the record may be disseminated to a Federal, state, local or foreign agency, or to an individual or organization, if there is reason to believe that such agency, individual or organization possesses information relating to the investigation, trial or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or informant; (3) a record relating to a case or matter may be disseminated in an appropriate Federal, state, local or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practice; (4) a record relating to a case or matter may be disseminated to a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing; (5) a record relating to a case or matter may be disseminated to an actual or potential party or attorney for the purpose of negotiation or discussion of such matters as settlement of the case or matter, plea bargaining, or formal or informal discovery proceedings; (6) a record relating to a case or matter that has been referred by an agency for investigation, prosecution, or enforcement, or that involves a case or matter within the jurisdiction of an agency, or where the agency or officials thereof are a party to litigation or where the agency or officials may be

affected by a case or matter, may be disseminated to such agency to notify the agency status of the case or matter or of any decision or determination that has been made, or such other inquiries and reports as are necessary during the processing of the case or

(7) a record relating to a person held in custody pending or during arraignment, trial, or extradition proceedings, or after conviction or after extradition proceedings, may be disseminated to a Federal, state, local or foreign prison, probation, parole, or pardon authority or to any other agency or individual concerned with the maintenance, transportation, or care of such a person; (8) a record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States or to an executive agreement; (9) a record may be disseminated to a Federal, state, local, foreign, or international law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency; (10) a record may be disseminated to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter; (11) a record may be disseminated to the public, news media, trade associations, or organized groups, when the purpose of the dissemination is educational or informational, provided that the record does not contain information identifiable to a specific individual other than is necessary to identify the matter where the information has previously been filed in a judicial or administrative office, including the clerk of the court; (12) a record may be disseminated to a foreign country, through the United States Department of State or directly to the representative of such country, to the extent necessary to assist such country in civil or criminal proceedings in which the United States or one of its officers or agencies has an interest; (13) a record that contains classified national security information and material may be disseminated to persons who are engaged in historical research projects, or who have previously occupied policy making positions to which they were appointed by the President, in accordance with the provisions of 28 CFR 17.6; (14) records are also available to the public for inspection and distribution as set forth at 8 CFR 503.1, including (a) Annual Reports of the Office of Alien Property, and (b) final determination opinions and orders in cases heard or reviewed within the Office of Alien Property; (15) records and documents are available for inspection by persons properly and directly concerned with the connection with claims filed with the Office, records in cases heard or reviewed in the Office and authorizations for sale and records of bids in public sales and orders for their acceptance or rejection and notifications thereof; (16) any record or portion thereof may also be disseminated to the Department of the Treasury and to the Foreign Claims Settlement Commission as a matter of routine use when such record relates to matters within the

jurisdiction of the Office of Foreign Assets Control, Department of the Treasury, or claim processed before the Foreign Claims Settlement Commission; (17) any record or portion thereof relating to an estate or trust matter under the jurisdiction of the probate courts of several states may be disseminated to the parties and their representatives or to the courts in proceedings involving the property owned or claimed to have been owned by a designated national of an enemy country under the provisions of the Trading with the Enemy Act; (18) a record may be disseminated to the Department of State for any negotiation or other activity relating to the Office of Alien Property or to any subject matter which is, or was at one time, under the jurisdiction of the Office of Alien Property.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Information in the system is stored in standard file jackets, and on index cards, within standard filing cabinets.

Retrievability:

The files and index cards must be retrieved by file numbers, which can be ascertained from alphabetical indices if the name of the non-government party is known, or from numeric indices relating to the various vesting orders, accounts, claims, or cases.

Safeguards:

Information in the system is regarded as confidential, pursuant to 8 CFR 503.17. Departmental rules and procedures are in force that insure that only Departmental attorneys and their authorized agents have access to this information.

Retention and disposal:

A file is closed when one of the following occurs:

1. The vesting order has been complied with and the property disposed of pursuant to the Trading with the Enemy Act, and all claims have been processed.
2. A case involving the Office of Alien Property has ended by the final termination of the litigation through a compromise settlement, court decision or any other method of termination for court cases.

The file is then retained in the Federal Records Center for a number of years and thereafter may be destroyed. Index cards are retained for as long as may be practicable.

System manager(s) and address:

Assistant Attorney General, Civil Division, U.S. Department of Justice, 10th and Constitution

Avenue, NW, Washington, DC 20530.

Notification procedure:

Address inquiries to Assistant Attorney General, Civil Division, U.S. Department of Justice and Constitution Avenue, NW, Washington, DC 20530.

Record access procedures:

A request for access to a record within the Office of Alien Property system involving material privacy and which is not otherwise available to the party requesting the same should be submitted in writing, with the envelope and letter clearly marked "Privacy Access Request." The request should include file or account numbers and/or the names of any known non-government parties. The requestor should also provide a return address for transmission of the information. Such access requests should be submitted to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above. The request should clearly state what information is being contested, the reasons for contesting it and the proposed amendment to the information sought.

Record source categories:

All claimants to property, as well as former depositories, are sources of information, also offices and agencies operating under provisions of the Trading with the Enemy Act.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/CIV-004

System name:

Swine Flu Administrative Claim File System.

System location:

Civil Division, U.S. Department of Justice 521 12th Street NW, No. 804, Washington, DC 20530.

Categories of individuals covered by the system:

Any and all parties making administrative claims for damages resulting from the administration of the swine flu vaccine, whose claims have been referred by the Department of Health, Education, and Welfare for handling by the Civil Division, will have identifying data contained in this system.

Categories of records in the system:

(1) The main record of the system is the administrative claim file which is retained on each claim under the jurisdiction of the Civil Division and constitutes the official record of the Department of Justice. All record material relating to a claim is retained in the file. Each claim is assigned a number in sequential order from the date of the filing. (2) Alphabetical and numerical indices are utilized as a means of access to the proper file by the cross-referencing of the names of all claimants with the file number. Index cards are used in these indices. A Docket Card Index is maintained on each claim in order to follow the progress of all swine flu claims and to obtain statistical data for periodic and fiscal reports. However, all information contained on the cards has been taken from the record material contained in the official

Authority for maintenance of the system:

General authority to maintain the system is contained in 5 U.S.C. 301 and 44 U.S.C. 3105. A particular system was established by authority of 28 CFR 0.77(f) which authority was delegated to the Civil Division pursuant to a memorandum from the Deputy Attorney General, dated May 17, 1974.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Any record pertaining to any swine flu administrative claim in the Civil Division may be disseminated to any other component of the Department of Justice, including the FBI and United States Attorneys' Offices, for use in connection with the consideration of that claim matter or any other claim, case or matter under consideration by the Civil Division or any component of the Department of Justice. A record maintained in this system of records disseminated as a routine use of such record as follows: (1) A record relating to a claim matter that has been referred by the Department of Health, Education, and Welfare for investigation, or that involves a claim or matter within the jurisdiction of an agency, or where an agency or officials thereof are a party to litigation or where the agency or officials may be affected by a claim or matter may be disseminated to such agency to notify the agency status of the claim or matter or any decision or determination that has been made, or to respond to such other inquiries and reports as are necessary during the processing of the claim or (2) a record may be disseminated to the public, news media, trade associations, or other groups, when the purpose of the dissemination is educational or informational, provided the record does not contain any information identifiable to a specific individual other than as necessary to identify the matter and is not an unwarranted invasion of privacy or where the information has previously been filed in a judicial or administrative office, including the court; (3) in any claim in which there is an indication of a violation or potential violation of law, whether civil, criminal or regulatory in nature, the record in question may be disseminated to the appropriate federal, state, local or foreign agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law; (4) in the course of investigating the potential or actual violation of any law, whether civil, criminal or regulatory in nature, or during the course of a trial or hearing, or the preparation for a trial or hearing for such violation, a record may be disseminated to a federal, state, local or foreign agency, or to an individual or organization, if there is reason to believe that such agency, individual or organization possesses information relating to the investigation, trial or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant; (5) a record relating to a claim or matter may be disseminated in an appropriate federal, state, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practice; (6) a record relating to a claim or matter may be disseminated to a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing; (7) a record relating to a claim or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion of such matters as settlement of the claim or matter, or for formal or informal discovery proceedings.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information of Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

(1) The claim files utilize standard file jackets and are retained in standard file cabinets; alphabetical and numerical index cards, as well as the docket cards, are retained in standard file cabinets.

Retrievability:

The files and docket cards must be retrieved by file number. The file number can be

ascertained from the alphabetical index if the name of the administrative claimant is known.

Safeguards:

Information contained in the system is unclassified. No personalized information about a claimant or claimant will be given to anyone other than the claimant, his attorney, or authorized representative. Requests for such information will not be given by telephone unless the requester can provide sufficient information to identify himself as one authorized to receive personal information. Nonpersonal or generalized information will be given to any requester. Information in the system is regarded as sensitive pursuant to Department rules and procedures. Department rules and procedures are in force to insure that only Departmental attorneys and their authorized agents have access to the information.

Retention and disposal:

When a claim file is closed by the legal section, it is sent to the Federal Records Center for retention in accordance with the authorized Record Disposal Schedule for the classification of the case. Such schedules are approved by the National Archives. After the designated retention period has passed, the file is destroyed. However, the index and docket cards are not purged and are retained for as long as practicable.

System manager(s) and address:

Assistant Attorney General, Civil Division, U.S. Department of Justice, 10th and Constitution Avenue NW, Washington, DC 20530.

Notification procedure:

Address inquiries to Chief, Torts Section, Civil Division, U.S. Department of Justice, 10th Constitution Avenue NW, Washington, DC 20530.

Record access procedures:

A request for information concerning the swine flu administrative claims of the Civil Division should be submitted in writing, with the envelope and letter clearly marked "Privacy Act Request". The request should include the file number and/or names of any claimants known to the requester. The requester should also provide a return address for transmitting the

information. Such access requests should be submitted to the System Manager listed a Requests may also be made by telephone. In such cases the caller will be referred to the attorney of record. The attorney, in turn, may require an official written request.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above. The request should clearly state what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

All swine flu claimants are sources of information. Such information is either contained in record material in the case files or has been extracted from that record material and put in docket and index cards.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/CIV-005

System name:

Annuity Brokers List System.

Security classification:

None.

System location:

Civil Division, U.S. Department of Justice, 950 Pennsylvania Avenue, NW., Washington, 20530; Department of Justice—Records Management Unit, 2711 Prosperity Avenue, Fairfax, Virginia 22031.

VA 22031; and Federal Records Center, Suitland, MD 20409.

Categories of individuals covered by the system:

Individuals who are seeking to be included in the list of annuity brokers mandated by section 11015 of the "21st Century Department of Justice Appropriations Authorization Act."

Categories of records in the system:

Records in this system include: declarations filed by annuity brokers and associated correspondence.

Authority for maintenance of the system:

Pub. L. 107-273, 21st Century Department of Justice Appropriations Authorization Act, section 11015(a).

Purpose(s):

These records are collected and maintained for the purpose of establishing a list of annuity brokers who meet minimum qualifications for providing annuity brokerage services in connection with structured settlements entered by the United States.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

None.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining and disposing of records in the system:

Storage:

Paper records are maintained in filing cabinets. Automated data, including records that

been transformed into electronic form, are stored on computer discs or magnetic tapes, are also stored in cabinets.

Retrievability:

Files and automated data are retrieved by name of an individual.

Safeguards:

Files and automated data are maintained under supervision of Civil Division personnel and contractors. During working hours—only authorized personnel, with the appropriate authorization, may handle, retrieve, or disclose any information contained therein. Access to electronic records is controlled by password or other user identification code.

Retention and disposal:

A request for authority to maintain and dispose of annuity broker list records has been submitted to the National Archives and Records Administration and is pending. In the interim, all records received will be retained and no records will be destroyed.

System manager(s) and address:

Office of the Assistant Attorney General, Civil Division, 950 Pennsylvania Avenue, NW., Washington, DC 20530.

Notification procedures:

Address inquiries to: Office of the Assistant Attorney General, Civil Division, 950 Pennsylvania Avenue, NW., Washington, DC 20530.

Record access procedures:

Individuals seeking access to information about their records may write to the Office of the Assistant Attorney General, Civil Division, 950 Pennsylvania Avenue, NW., Washington, DC 20530. The request should state what records are sought and must include the requestor's name and current address. The request must be signed before a notary or signed, dated, and submitted under penalty of perjury.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the Office of the Assistant Attorney General, Civil Division, 950 Pennsylvania Avenue, NW., Washington, DC 20530. The request should clearly and concisely state what information is being contested, the reason(s) for contesting it, and the proposed amendment to the record.

Record source categories:

Individuals submitting information who are seeking to be included in the Department of Justice list of annuity brokers.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/CIV-006

System name:

Consumer Inquiry/Investigatory System.

System location:

Civil Division, U.S. Department of Justice, 666 11th Street NW, Washington, DC 20530.

Categories of individuals covered by the system:

Individuals with complaints or inquiries on consumer matters.

Categories of records in the system:

The records consist of complaints and inquiries from private individuals, any replies thereon, other correspondence and internal memoranda related to the investigation of such inquiries.

violations of criminal or civil Federal law.

Authority for maintenance of the system:

U.S.C. 3101; 5 U.S.C. 301.

Purpose(s):

These records are maintained for the purpose of responding to consumer complaints or inquiries and to further or initiate investigations for law enforcement purposes.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

(1) A complaint/inquiry, or any information developed in response thereto may be disclosed to other Federal, State or local agencies for law enforcement purposes, to ensure completion of the matter, or to better assess consumer-related problems and programs.

(2) A complaint/inquiry or any information derived therefrom may be disclosed to a private individual who is the subject of a complaint/inquiry to resolve the issues raised in the complaint/inquiry and to fulfill the Department's law enforcement responsibilities.

(3) To facilitate processing Freedom of Information and Privacy Act requests for these records, a record may be disclosed to another Federal agency to (a) permit a decision as to access, amendment or correction of records to be made in consultation with or by that agency or (b) to verify the identity of an individual or the accuracy of information submitted by an individual who has requested access to, or amendment or correction of records.

(4) A record or information derived therefrom may be released to the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release would constitute an unwarranted invasion of personal privacy.

(5) A record may be disclosed to the National Archives and Records Administration and General Services Administration to conduct records management inspections authorized by U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose

relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

These records are stored in file folders in cabinets.

Retrievability:

Information is retrieved by name subject matter and date.

Safeguards:

Information contained in the system is unclassified. During duty hours access to this system is monitored and controlled by Civil Division personnel in the area where the system is maintained. The area is locked during non-duty hours.

Retention and disposal:

In accordance with the General Record Schedule 14, item 6, records are retained for one year after close of the file or completion of the project, after which the files are destroyed.

System manager(s) and address:

Assistant Attorney General, Civil Division, U.S. Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Address inquiries to the Assistant Attorney General, Civil Division, Department of Justice

and Constitution Avenue, NW, Washington, DC 20530.

Record access procedures:

A request for access to a record from this system shall be written and clearly identified as "Privacy Access Request." The request should include the name of the party making the inquiry and the date of the inquiry. The requester should indicate a return address. The request should be directed to the system manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should state clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. The request should be directed to the system manager listed above.

Record source categories:

Sources of records maintained in the system are the public inquiries, and information provided by private firms regarding the subject matter of such inquiries.

Systems exempted from certain provisions of the act:

The Attorney General has exempted certain categories of records in this system from subsections (c) (3) and (4), (d), (e)(1) and (e)(5) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k) (2). That is, these exemptions apply only to the extent that the file contains records combined for civil or criminal law enforcement purposes. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

Justice/CIV-008

System name:

September 11th Victim Compensation Fund of 2001 File System.

Security classification:

None.

System location:

Civil Division, U.S. Department of Justice, 950 Pennsylvania Avenue, NW., Washington, 20530; Department of Justice—Records Management Unit, 2711 Prosperity Avenue, Fairfax, VA 22031; and Federal Records Center, Suitland, MD 20409.

Categories of individuals covered by the system:

Individuals who claim benefits under the September 11th Victim Compensation Fund of 2001 (i.e. individuals claiming to have suffered physical injury or the personal representatives of individuals who were killed as a result of the terrorist-related aircraft crashes of September 11, 2001).

Categories of records in the system:

Records in this system include: Claim forms filed by or on behalf of claimants seeking benefits under the Fund; documents submitted in support of the claims; medical, personal, employment, financial, and other records obtained or generated to adjudicate the claims.

Authority for maintenance of the system:

September 11th Victim Compensation Fund of 2001 enacted into law as Title IV of Pub. Law 107-42, 115 Stat. 230 ("Air Transportation Safety and System Stabilization Act").

Purpose(s)

These records are collected or generated for the purpose of determining qualification of claimants for compensation to claimants under the September 11th Victim Compensation Fund of 2001.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

It is likely that routine uses will be published at a later date with an opportunity for comment.

the interim, disclosures necessary to process claims will be made only with the written consent of claimants.

Disclosures to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining and disposing of information in the system:

Storage:

Paper case files are maintained in filing cabinets. Automated data, including case files that have been transformed into electronic form, are stored on computer discs or magnetic tape, which are also stored in cabinets.

Retrievability:

Files and automated data are retrieved by name of a claimant or personal representative of a claimant, the name of the deceased, case file number and/or Social Security Number.

Safeguards:

Files and automated data are maintained under supervision of Civil Division personnel, Special Master, or their contractors. During working hours—only authorized personnel, with appropriate password may handle, retrieve, or disclose any information contained therein. Access to electronic records is controlled by password or other user identification code.

Retention and disposal:

All claim files and automated data pertaining to a claim are destroyed 10 years after the claim has been fully adjudicated and/or payment made, as approved by the National Archives and Records Administration. Paper files that have been scanned to create electronic copies may be destroyed after the copies are verified. Automated data is retained in its current form only, however, and as information is updated, outdated information is deleted.

System manager(s) and address:

Office of the Assistant Attorney General, Civil Division, 950 Pennsylvania Avenue, NW,
Washington, DC 20530.

Notification procedure:

Address inquiries to: Office of the Assistant Attorney General, Civil Division, 950 Pennsylvania Avenue, NW, Washington, DC 20530.

Record access procedures:

Any individual seeking access to information about a claim in which he/she is a party in may write to the Office of the Assistant Attorney General, Civil Division, 950 Pennsylvania Avenue, NW, Washington, DC 20530. The request should state what records are sought must include the requester's full name, current address, and claim file number (if known). The request must be signed before a notary or submitted under penalty of perjury.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the Office of the Assistant Attorney General, Civil Division, 950 Pennsylvania Avenue, NW, Washington, DC 20530. The request should clearly and concisely state what information is being contested, the reason(s) for contesting it, and the proposed amendment to the record.

Record source categories:

Individuals or entities having information pertinent to the adjudication of compensation claims including but not limited to: Injured individuals; personal representatives of deceased individuals; eligible claimants; family members; physicians and other medical professionals; hospitals, and clinics; insurers, employers, and their agents and representatives.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

Civil Rights Division

JUSTICE/CRT-001

System name:

Central Civil Rights Division Index File and Associated Records, CRT-001.

System location:

United States Department of Justice, Civil Rights Division (CRT), 950 Pennsylvania Avenue NW., Washington, DC 20530-0001.

Categories of individuals covered by the system:

These persons may include: Subjects of investigations, victims, potential witnesses, and individuals of Japanese ancestry who were eligible, or potentially eligible, for restitution benefits as a result of their evacuation, relocation, or internment during World War II, and representatives on behalf of individuals and other correspondents on subjects directed or referred to CRT (including persons or organizations referred to CRT in potential or actual cases and matters of concern to CRT), and CRT employees who handle complaints, cases or matters of concern to CRT.

Categories of records in the system:

Records in this system consist of case files, matters, memoranda, correspondence, studies, and reports relating to enforcement of civil rights laws and other various duties of the Civil Rights Division. The delegated legal duties and responsibilities of each section are described in detail at the Civil Rights Division Web page: <http://www.usdoj.gov/crt/crt-home.aspx>. In addition to the sections, the Civil Rights Division maintains records related to the duties of the Office of Redress Administration pertaining to the identification, location and authorization of restitution payments to eligible individuals of Japanese ancestry who were evacuated, relocated or interned during World War II. These restitution payments were authorized by section 105 of the Civil Liberties Act of 1988 (50 U.S.C. App. 1989b). Finally, the names of some individuals, e.g., witnesses, may not yet be on the central indices and may be obtained by direct access to the file jackets. Such file jackets are located within the respective sections of CRT according to the legal subject matter assigned to each CRT section.

Authority for maintenance of the system:

The records in the system of records are kept under the authority of 44 U.S.C. 3101 and the ordinary course of fulfilling the responsibility assigned to CRT under the provisions of 28 U.S.C. 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000.

Purpose(s):

The purposes of this system are to assist all the sections within the Division in maintaining names of Division employees and their case investigation assignments, names of defendants or investigation targets, victims, witnesses or potential witnesses, or other persons or organizations as they relate to potential or actual cases, investigations, and matters of concern to CRT. Other purposes are to assist employees and officials within the Division to review and make decisions in the course of investigations and legal proceedings, to assist the Division in preparing budget requests, to respond to inquiries from outside the Department, and to carry out other authorized Department functions.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of the system of records as follows:

(1) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, foreign, or Tribal law enforcement authority or other appropriate agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing the law;

(2) In the course of the administration by CRT of a federally mandated program, or the investigation or litigation of a case or matter, a record may be disseminated to a Federal, State, or local agency, or to an individual or organization, if there is reason to believe that such agency, individual or organization possesses information or has the expertise in an official or technical capacity to assist in the administration of such program or to analyze information relating to the investigation, trial or hearing and the dissemination is reasonably necessary.

elicit such assistance, information or expert analysis, or to obtain the cooperation of a prospective witness or informant;

(3) A record relating to a case or matter, or any facts derived therefrom, may be disseminated in a proceeding before a court, grand jury, administrative or regulatory proceeding or an adjudicative body before which CRT is authorized to appear, when the United States, or agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(4) A record relating to a case or matter may be disseminated to an actual or potential party to litigation or the party's attorney (a) for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining or (b) in informal discovery proceedings;

(5) A record relating to a case or matter that has been referred for investigation may be disseminated to the referring agency to notify such agency of the status of the case or matter or of any determination that has been made;

(6) A record relating to a person held in custody or probation during a criminal proceeding after conviction may be disseminated to any agency or individual having responsibility for the maintenance, supervision or release of such person;

(7) A record may be disseminated to the United States Commission on Civil Rights in response to its request and pursuant to 42 U.S.C. 1975d;

(8) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;

(9) A record may be disseminated to mediators, negotiators or other persons engaged in efforts to resolve or settle cases or matters pending in the Division as is necessary to enable them to perform their assigned duties;

(10) A record may be disseminated to complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress or results of the investigation or case arising from the matters of which the complainants or victims

complained or of which they were a victim;

(11) Information relating to health care fraud may be disclosed to private health plans, c associations of private health plans, health insurers, or associations of health insurers, t promote the coordination of efforts to prevent, detect, investigate, and prosecute health fraud; to assist efforts by victims of health care fraud to obtain restitution; to enable priv health plans to participate in local, regional, and national health care fraud task force ac and to assist tribunals, which have jurisdiction over claims against private health plans f allegedly improper disclosures to the Department of Justice of information concerning suspected health care fraud, in determining whether the private health plan qualifies for statutory immunity from civil liability as provided by Section 201 of the Health Insurance Portability and Accountability Act of 1998, codified at 42 U.S.C. 1320a-7c(a)(3)(B)(iii);

(12) Information permitted to be released to the news media and the public pursuant to 50.2 may be made available unless it is determined that release of the specific informati the context of a particular case would constitute an unwarranted invasion of personal pr

(13) Information may be disclosed as is necessary to respond to inquiries by Members c Congress on behalf of individual constituents who are subjects of CRT records;

(14) A record may be disclosed as a routine use to the National Archives and Records Administration (NARA) and to the General Services Administration (GSA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(15) To a former employee of the Department for purposes of: Responding to an official by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with former employee that may be necessary for personnel-related or other official purposes the Department requires information and/or consultation assistance from the former em regarding a matter within that person's former area of responsibility.

(16) To the local community or public when the incident investigated has become a mat public knowledge, the investigation is closed, and the Assistant Attorney General, Civil l Division, personally determines that, because there is a reasonable potential for civil un a severe loss of confidence by the public in the investigative process, the disclosure of information explaining the Department's decision to close a criminal matter is appropriat

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Information in this system is stored on index cards, in file jackets, and on computer disk tapes.

Retrievability:

Records are retrieved by the names of individuals or by case numbers assigned to certain cases being investigated by the Department.

Safeguards:

Information in manual and computer form is safeguarded and protected in accordance with applicable Department security regulations for systems of records. Only a limited number of staff members who are assigned a specific identification code will be able to use the code to access the stored information. However, a section may decide to allow its employees access to the system in order to perform their official duties.

Retention and disposal:

Records are maintained on the system while current and required for official Government use. When no longer needed on an active basis, the paper files are transferred to the Federal Records Center, Suitland, Maryland and some records are transferred to computer tape and stored in accordance with Department security regulations for systems of records. Final disposition is in accordance with records retention schedules approved by NARA.

System manager(s) and address:

Executive Officer, Administrative Management Section, Civil Rights Division, United States Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001.

Notification procedure:

Part of this system is exempted from this requirement under 5 U.S.C. 552a(j)(2) and (k).

Address inquiries to the System Manager listed above.

Record access procedures:

Part of this system is exempted from this requirement under 5 U.S.C. 552a(j)(2) and (k); to the extent that this system of records is not subject to exemption, it is subject to access contest. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record retrievable in this system shall be made in writing with the envelope and letter clearly marked "Privacy Access Request." Include in the request the full name of the individual, his or her current address, date and place of birth, notarized signature or dated signature submitted under penalty of perjury (28 CFR 16.41(d)), the title of the case or matter as described under "Categories of records in the system," and any other information which is known and may be of assistance in locating the record, such as the title of the civil rights related case or matter involved, where and when it occurred and the name of the judicial district involved. The requester will also provide a return address for transmission of the information. Access requests should be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend non-exempt information retrievable in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in this system may be an agency or person who has confidential information related to the law enforcement responsibilities and/or other statutorily-mandated duties of CRT.

Exemptions claimed for the system:

The Attorney General has exempted parts of this system from subsections (c)(3) and (4)(d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*. These exemptions apply only to the extent that information in a record pertaining to a person

individual relates to an official federal investigation and/or law enforcement matter. Those indexed under an individual's name which concern only the administrative management restitution payments under section 105 of the Civil Liberties Act of 1988 are not being ex pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

[\[TOP\]](#)

JUSTICE/CRT-002

System name: Files of Applications for the Position of Attorney with the Civil Rights Division.

System location:

U.S. Department of Justice, Civil Rights Division (CRT), 10th and Constitution Avenue, N
Washington, DC 20530.

Categories of individuals covered by the system:

Persons who have applied for a position as an attorney with CRT.

Categories of records in the system:

The system may contain SF 171 forms, resumes, referral letters, letters of recommendation writing samples, interview notes, internal notes or memoranda, and other correspondence documents.

Authority for maintenance of the system:

The records in this system of records are kept under the authority of 44 U.S.C. 3101 and ordinary course of fulfilling the responsibilities assigned to CRT under 28 CFR 0.50, 0.5

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The records in this system are used by employees and officials of the Department in making employment decisions. If an individual is hired, the records may become part of his or her

Official Personnel Folder.

A record relating to this system, or any facts derived therefrom, may be disseminated in proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which the Civil Rights Division is authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by the Civil Rights Division to be arguably relevant to the litigation. A record relating to this system may be disseminated to an actual or potential party to litigation or the party's attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining or in formal or informal discussions or proceedings.

Release of information to the news media: Information permitted to be released in the news media and the public pursuant to 28 CFR 50.2 may be made available from systems or records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information of Members of Congress. Information in the system may be disclosed if it is necessary to respond to inquiries by Members of Congress on behalf of individual constituents that are subjects of CRT records.

Release of information to the National Archives and Records Administration: A record from this system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records in the system are primarily original papers or reproductions or copies thereof. The system consists of files pertaining to individual applicants.

Retrievability:

Information is retrieved by using an applicant's name.

Safeguards:

Information in the system is unclassified. It is safeguarded and protected in accordance with Departmental rules and procedures governing access, production and disclosure of any materials contained in its official files.

Retention and disposal:

Information is retained in the system until a final employment decision is made or until such time as CRT is notified by the applicant that he or she is no longer interested in or available for the position. If an individual is hired, some or all of the records may become part of his or her Official Personnel Folder.

System manager(s) and address:

Deputy Assistant Attorney General, Civil Rights Division, U.S. Department of Justice, Washington, DC 20530.

Notification procedure:

Address inquiries to the Assistant Attorney General, Civil Rights Division, U.S. Department of Justice, Washington, DC 20530.

Record access procedures:

A request for access to a record from this system shall be made in writing with the envelope and the letter clearly marked 'Privacy Access Request.' The request should include the name of the applicant and the position applied for. The requester will also provide a return address.

for transmitting the information. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in the system generally are the applicants, persons recommending the applicant, and employees and officials of the Department.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/CRT-003

System name:

Civil Rights Interactive Case Management System (ICM).

System location:

United States Department of Justice, Civil Rights Division (CRT), 950 Constitution Ave., Washington, DC 20530-0001.

Categories of individuals covered by the system:

These persons may include: Complainants, victims, defendants, parties, experts, media, Assistant U.S. Attorneys, judges, and individuals or representatives on behalf of individuals in potential or actual cases and matters of concern under jurisdiction of the Civil Rights Division.

and CRT employees, including attorneys, paralegals, and professional staff, who handle complaints, cases or matters of concern to CRT.

Categories of records in the system:

- (1) Records in this system pertain to a broad variety of cases and matters under the jurisdiction of the CRT relating to disability rights, education, employment, housing, special litigation, voting, criminal, enforcement, and other civil rights laws or matters;
- (2) Summary information of these cases or matters is maintained in the system including information as names of principal parties or subjects, proper case name, case numbers, judicial district, assignments, alleged violation, section of CRT responsible for the matter, case status, ranging from the preliminary development stage, through investigation, litigation, compliance, appeal, conviction or closure; and
- (3) The ICM also has a time reporting system that allows the CRT to capture, analyze and report the professional time attorneys, paralegals and other employees of the Division spend on investigation and case related tasks.

Purpose(s):

The ICM is designed to track, count and measure all investigations and cases throughout the life cycle. The CRT uses reports generated from this system to provide a profile for each section's activities and to furnish management with a global perspective to the CRT work. The ICM also has a time reporting system that allows the CRT to capture, analyze and report the level of effort attorneys, paralegals, and professional staff spend on investigation and related tasks. One purpose of this system is to assist employees and officials of the Department to keep track of resources and professional time devoted to individual assignments to matters and broad categories of cases. Another purpose is to assist the CRT in preparing budget requests and other reports which may be submitted to the Attorney General or to Congress.

Authority for maintenance of the system:

The records in this system are kept under the authority of 44 U.S.C. 3101 and in the course of fulfilling the responsibilities assigned to CRT under 28 CFR 0.50, 0.51.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of records as follows:

(1) A record relating to this system, or any facts derived therefrom, may be disseminated proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is authorized to appear, when the United States, or agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(2) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, federal or Tribal law enforcement authority or other appropriate agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing the law;

(3) A record relating to this system may be disseminated to an actual or potential party to litigation or the party's attorney or authorized representative for the purpose of negotiating a discussion on such matters as settlement of the case or matter, plea bargaining, or in its discovery proceedings;

(4) A record may be disseminated to contractors, grantees, experts, consultants, students or others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(5) A record may be disseminated to complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress or results of the investigation or case arising from the matters of which the complainants or victims complained or of which they were a victim;

(6) A record may be disseminated to a former employee of the Department for purposes of responding to an official inquiry by a Federal, State, or local government entity or professional

licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(7) Information permitted to be released to the news media and the public pursuant to 28 U.S.C. 50.2 may be made available unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(8) Information in the system may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents who are subjects of CRT records and

(9) A record from the system or records may be disclosed to National Archives and Records Administration (NARA) and General Services Administration (GSA) for records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are maintained electronically in the ICM computerized information system.

Retrievability:

Information is retrieved by name or other identifier assigned to an individual.

Safeguards:

Information contained in the system is unclassified. It is safeguarded and protected in accordance with Departmental security regulations for systems or records. Access to the records is limited to those employees whose official duties require such access in order to perform their duties.

Retention and disposal:

Records are maintained in the system while current and required for official Government use. When no longer needed on an active basis, the records are stored in accordance with Departmental security regulations for systems of records. The disposition schedule is pending approval at NARA.

System manager(s) and address:

Executive Officer, Administrative Management Section, Civil Rights Division, United States Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001.

Notification procedure:

Address inquiries to the system manager listed above.

Record access procedures:

A request for access to a record retrievable in this system shall be made in writing, with envelope and letter clearly marked "Privacy Access Request." Include in the request the name of the individual involved, his or her current address, date and place of birth, and notarized signature or dated signature submitted under penalty of perjury (28 CFR 16.4) and any other information which is known and may be of assistance in locating the record. The requester should provide a return address for transmitting the information. Access requests should be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend their records should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Information on time-allocation is provided by CRT attorneys, paralegals and professionals who handle complaints, cases or matters of concern to the CRT. Sources of information contained in this system are those records reflecting all cases or matters under consideration by CRT.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

JUSTICE/CRT-004

System name:

Registry of Names of Interested Persons Desiring Notification of Submissions under Section 5 of the Voting Rights Act.

System location:

U.S. Department of Justice, Civil Rights Division (CRT), 950 Pennsylvania Avenue, NW. Washington, DC 20530-0001.

Categories of individuals covered by the system:

Persons who have requested that the Attorney General send them notice of submission under Section 5 of the Voting Rights Act of 1965, 42 U.S.C. 1973c.

Categories of records in the system:

The Registry contains the name, address and telephone numbers of interested parties, where appropriate, the voting area or areas with respect to which notification was requested from such persons.

Authority for maintenance of the system:

46 FR 877 (1981) codified in 28 CFR part 51, 42 U.S.C. 1973c, 5 U.S.C. 301 and 28 U.S.C. 509, 510.

Purpose(s):

The purpose is to maintain records in a Registry to identify persons interested in receiving

notification of submissions under Section 5 of the Voting Rights Act and to comply with requests. Section 5, which applies to several states and some counties, requires that any change with respect to voting that a specially covered jurisdiction makes is legally unenforceable unless and until the jurisdiction obtains from the Federal court in the District of Columbia or from the Attorney General a determination that the change is not discriminatory on account of race, color, or membership in a language minority group. If the jurisdiction is unable to prove the absence of discrimination, the Attorney General objects to the change, and the change remains legally unenforceable. Further, the Registry may be used to notify the persons within the jurisdiction of any proposed changes in the "Procedures for the Administration of Section 5 of the Voting Rights Act of 1965," 46 FR 870 (1981), codified in 28 CFR part 51, and to solicit their comments with respect to any such proposed changes.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of the system of records as follows:

(1) A record relating to this system, or any facts derived therefrom, may be disseminated in any proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(2) A record relating to this system may be disseminated to an actual or potential party to litigation or the party's attorney or authorized representative for the purpose of negotiating a settlement of the case or matter, plea bargaining or in discovery proceedings.

(3) A record may be disseminated to contractors, grantees, experts, consultants, students or others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(4) A record may be disseminated to complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which the complainants or victims

complained or of which they were a victim;

(5) Information permitted to be released to the news media and the public pursuant to 25 U.S.C. 50.2 may be made available from systems of records maintained by the Department of Justice, unless it is determined that release of the specific information in the context of a particular request would constitute an unwarranted invasion of personal privacy;

(6) Information in the system may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents who are subjects of CRT records;

(7) A record from a system of records may be disclosed as a routine use to National Archives and Records Administration (NARA) and General Services Administration (GSA) in record management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(8) A record may be disclosed to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility and

(9) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, or tribal law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Names are stored in a card file system, and an automated addresser.

Retrievability:

Records in this system are retrievable by the names of interested persons or organizations.

Safeguards:

Information in the system is safeguarded in accordance with Departmental rules and procedures governing access, production and disclosure of any materials contained in its official files.

Retention and disposal:

An individual or organizational name is retained in the Registry until such time as that person or organization requests that the name be deleted.

System manager(S) AND ADDRESS:

Chief, Voting Section, Civil Rights Division, U.S. Department of Justice, 950 Pennsylvania NW., Washington, DC 20530-0001.

Notification procedure:

Address inquiries to: Assistant Attorney General, Civil Rights Division, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001.

Record access procedures:

This system contains no information about any individual other than as described in Categories of Records above. Persons whose names appear on the Registry may have access thereto. They may have their names and other information pertaining to them deleted or modified upon a request of the same nature as indicated in 46 FR 877 (1981), codified in 28 CFR part 51.

Contesting record procedures:

Same as the above.

Record source categories:

Sources of information in the Registry are those persons or organizations whose names

therein by virtue of their having requested inclusion in the Registry pursuant to 46 FR 8 (1981), codified in 28 CFR 51.32.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

JUSTICE/CRT-007

System name:

Files on Employment Civil Rights Matters Referred by the Equal Employment Opportunity Commission.

System location:

U.S. Department of Justice, Civil Rights Division (CRT), 950 Pennsylvania Avenue NW., Washington, DC 20530-0001.

Categories of individuals covered by the system:

Persons seeking employment or employed by a state or a political subdivision of a state have filed charges alleging discrimination in employment with the Equal Employment Opportunity Commission (hereinafter EEOC) which have resulted in a determination by that there is probable cause to believe that such discrimination has occurred, and attempt EEOC at conciliation have failed.

Categories of records in the system:

The system may contain copies of charges filed with EEOC, copies of EEOC's "determination letters, letters of transmittal from and to EEOC, analyses or evaluations summarizing the charge and other materials in the EEOC file, internal memoranda, attorney notes, and copies of "right to sue" letters issued by CRT. The system may also contain charges related to allegations of employment discrimination by public employers filed by individual complainants which have been referred to the Department of Justice by EEOC pursuant to 42 U.S.C.

2000e–5(f) (1) or 5(f) (2), or to allegations of a pattern or practice of violations of the Equal Employment Opportunity Act by a public employer which have been referred to the Department of Justice by EEOC pursuant to 42 U.S.C. 2000e–6. If the Department has determined to initiate an investigation or litigate a matter referred by EEOC the records pertaining to that matter are not contained in the system. Such records and their routine uses are described under the notice for the system named: Central CRT Index File and Associated Records/CRT–001.

Authority for maintenance of the system:

The records in this system of records are kept under authority of 44 U.S.C. 3101 and in the ordinary course of fulfilling the responsibilities assigned to CRT under 28 CFR 0.50, 0.51.

Purpose(s):

One purpose of this system is to assist employees and officials of the Department to make decisions regarding the issuance of right to sue letters or make decisions regarding prosecutions of alleged instances of employment discrimination. Another purpose is to assist the Division in preparing budget requests, statistical reports, and other internal functions of the Department.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of the system records as follows:

(1) A record relating to this system, or any facts derived therefrom may be disseminated in a proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(2) A record relating to this system may be disseminated to an actual or potential party to litigation or the party's attorney or authorized representative for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining or in pre-discovery proceedings;

(3) A record may be disseminated to contractors, grantees, experts, consultants, students or others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(4) A record may be disseminated to complainants and victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which the complainants or victims complained or of which they were a victim;

(5) Information permitted to be released to the news media and the public pursuant to 28 U.S.C. 50.2 may be made available from systems of records maintained by the Department of Justice, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(6) Information in the system may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents who are subjects of CRT records;

(7) A record from a system of records may be disclosed as a routine use to National Archives and Records Administration (NARA) and General Services Administration (GSA) in record management inspections conducted under the authority of 44 U.S.C. 2904 and 2906; and

(8) A record may be disclosed to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information in the systems is stored on index cards, in file jackets, and in computer disk files and are maintained by the Employment Litigation Section, Civil Rights Division.

Retrievability:

Information is retrieved primarily by using the appropriate Department of Justice file number, the name of the charging party, or the state in which the alleged discrimination occurred through other logical queries to the computer based system.

Safeguards:

Information in manual and computer form is safeguarded and protected in accordance with applicable Departmental security regulations for systems of records. Staff members who are assigned a specific identification code will be able to use the computer or to access the information in order to perform their official duties.

Retention and disposal:

If the Department determines not to prosecute a matter referred by the EEOC, the records transmitted with the referral are returned to the EEOC. Other records in the system are for routine use by the Department and when no longer needed are sent to the Federal Records Center or are destroyed. Records are retained and disposed of in accordance with item 1 of the General Records Schedule 1 as approved by the Archivist of the United States.

System manager(s) and address:

Assistant Attorney General, Civil Rights Division, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001.

Notification procedure:

Same as the above.

Record access procedures:

A request for access to a record from this system shall be made in writing with the envelope and letter clearly marked "Privacy Access Request." The request should indicate the state where the alleged employment discrimination took place and the employer to which the request was related. The requester should also provide the full name of the individual involved, her current address, date and place of birth, notarized signature or dated signature submitted.

under penalty of perjury (28 CFR 16.41(d)), any other known information which may be assistance in locating the record, and a return address for transmitting the information. requests will be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Disclosure of part of the material in this system may be prohibited by 42 U.S.C. 2000e-5(b), 42 U.S.C. 2000e-8(e) and 44 U.S.C. 3510(b). Part of this system is exempted from access and contest under 5 U.S.C. 552a(k) (2).

Record source categories:

Sources of information in this system are charging parties, information compiled and maintained by EEOC, and employees and officials of the Department of Justice responsible for the disposition of the referral request.

Exemptions claimed for the system:

The Attorney General has exempted the system from 5 U.S.C. 552a (d)(1), (2), (3), and the Privacy Act pursuant to 5 U.S.C. 552a (k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e), and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/CRT-009

System name:

Civil Rights Division Travel Reports, CRT-009.

System location:

United States Department of Justice, Civil Rights Division (CRT), 950 Pennsylvania Avenue

NW., Washington, DC 20530–0001.

Categories of individuals covered by the system:

All persons who have filed travel authorization forms or travel voucher forms for official travel on behalf of CRT.

Categories of records in the system:

The Division's filing system contains information concerning travel expenditures which were recorded on travel authorization forms and travel voucher forms by CRT employees or other persons authorized to travel for CRT and submitted to the Budget and Finance Branch.

Authority for maintenance of the system:

The records in this system of records are kept under the authority of 44 U.S.C. 3101 and the ordinary course of fulfilling the responsibilities assigned to CRT under 28 CFR 0.50, 0.51.

Purpose(s):

One purpose of this system is to assist employees and officials of the Division to measure and track expenditures within the Division. Other purposes are to assist the Division in preparing reports within various sections to control and review expenditures.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of the system's records as follows:

(1) A record relating to this system, or any facts derived therefrom, may be disseminated in a proceeding before a court, grand jury, administrative or regulatory proceeding or any other adjudicative body before which CRT is authorized to appear, when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by CRT to be arguably relevant to the litigation;

(2) A record relating to this system may be disseminated to an actual or potential party to

litigation or the party's attorney or authorized representative for the purpose of negotiating a settlement of the case or matter, plea bargaining or in pre-trial discovery proceedings;

(3) A record may be disseminated to contractors, grantees, experts, consultants, students or others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(4) Information permitted to be released to the news media and the public pursuant to 28 U.S.C. 50.2 may be made available from systems of records maintained by the Department of Justice, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(5) Information in the system may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents who are subjects of CRT records;

(6) A record from a system of records may be disclosed as a routine use to National Archives and Records Administration (NARA) and General Services Administration (GSA) in record management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(7) A record may be disclosed to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility and

(8) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law-criminal, civil or regulatory in nature-the relevant records may be referred to the appropriate Federal, State, local, foreign or Tribal law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records are stored in hard copy and electronic form.

Retrievability:

Records in this system are retrieved by the names of those individuals identified under the caption "Categories of individuals covered by the system."

Safeguards:

Information in the system is unclassified. However, the records are protected in accordance with applicable Department security regulations for systems of records. Records are stored in locked cabinets and access to the computer is limited to those personnel who have a need-to-know access to perform their official duties.

Retention and disposal:

Records are maintained on the system while current and required for official Government business. When no longer needed on an active basis, the records are transferred to computer tape and stored in accordance with Departmental security regulations for systems of records. Final disposition will be in accordance with records retirement or destruction as scheduled by the General Records Schedule 9.

System manager(s) and address:

Executive Officer, Administrative Management Section, Civil Rights Division, United States Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001.

Notification procedure:

Same as the above.

Record access procedures:

Requests by former employees for access to records in this system may be made in writing with the envelope and letter clearly marked "Privacy Act Request." The request should be

state the dates on which official travel was taken. The requestor should also provide the name of the individual involved, his or her current address, date and place of birth, note signature or dated signature submitted under penalty of perjury (28 CFR 16.41(d)), any known information which may be of assistance in locating the record, and a return address transmitting the information. Access requests will be directed to the System Manager. For employees may request access by contacting the System Manager directly.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reason for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information are CRT employees and other authorized persons who file travel authorization and travel voucher forms.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

Community Relations Service

JUSTICE/CRS-001

System name:

Operational Data Information System.

System location:

Community Relations Service, U.S. Department of Justice, 550 11th Street NW, Washington DC 20530.

Categories of individuals covered by the system:

Conciliators and Mediators of the Community Relations Service of the U.S. Department of Justice.

Categories of records in the system:

The file contains the names of CRS employees, their case assignments, and the time allocated to each assignment. In addition, information reflecting the current status and handling of each case is included within the system.

Authority for maintenance of the system:

The file is established to effect the purposes of 42 U.S.C. 2000g-1, 2000g-3 (1970).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The file is used by CRS personnel as a basis for preparing daily, weekly, and monthly reports for internal management. It is also used by the Administrative Office to prepare efficiency analyses on CRS personnel. In addition, the file will be consulted in order to prepare budget requests and reports to the Associate Attorney General, the Attorney General, and Congress.

Release of Information to the News Media and the Public: Information from the system or records may be made available to the news media and the public, unless such release would violate 42 U.S.C. 2000g-2, or would constitute an unwarranted invasion of personal privacy.

Release of Information to Members of Congress: Information contained in the system, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record unless such release would violate 42 U.S.C. 2000g-2.

Release of Information to the National Archives and Records Administration: A record from the system of records may be disclosed to the National Archives and Records Administration.

(NARA) for records management inspections conducted under the authority of 44 U.S.C. and 2906, unless such disclosure would violate 42 U.S.C. 2000g-2.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Automated records are maintained on magnetic disk at the Department of Justice Data Management Service.

Retrievability:

Information is retrieved by a variety of key words including, but not limited to, the name of the employee, geographic location, and subject matter of the record.

Safeguards:

Information maintained in the system is safeguarded and protected in accordance with Department rules and procedures governing the handling of computerized information. Only individuals specifically authorized by the Director of CRS will have access to the computer through a single terminal located in an office occupied during the day and locked at night. Access to the information in the system will be limited to those CRS employees whose duties require such information.

Retention and disposal:

Records classified by the subject's name are retained until 60 days after the record subject leaves the employment of the Community Relations Service and are then deleted from the system.

system.

System manager(s) and address:

Deputy Director, Community Relations Service, U.S. Department of Justice, Todd Building
11th Street NW, Washington, DC 20530.

Notification procedure:

Address inquiries to Office of Chief Counsel, Community Relations Service, U.S. Department of Justice, 550 11th Street NW, Washington, DC 20530.

Record access procedures:

In all cases, requests for access to a record shall be in writing, by mail or in person. If request for access is made by mail, the envelope and letter shall be clearly marked "Privacy Act Request." The requester shall include a description of the record requested and, if known, the case file number(s). To identify a record relating to an individual, the requester must provide the individual's full name, date and place of birth, employee identification number, and employment and duty assignment station(s) while employed by the Community Relations Service.

Contesting record procedures:

Any individual desiring to contest or amend information maintained in the system should submit his or her request to the Deputy Director, Community Relations Service, U.S. Department of Justice, Todd Building, 550 11th Street NW, Washington, DC 20530. The request should clearly state what information is being contested, the reason for contesting, and the proposed amendment to the information.

Record source categories:

The records are prepared by the conciliator/mediator or, in exceptional cases, by his or her supervisor.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

Criminal Division

DEPARTMENT OF JUSTICE/CRM-001

SYSTEM NAME:

Criminal Division Index File Systems and Associated Records.

SECURITY CLASSIFICATION:

The system itself is, in whole sensitive and in part, classified to protect national security policy material. Within the unclassified part, items or records may have Limited Official Information national security/foreign policy classifications.

SYSTEM LOCATION:

U.S. Department of Justice, Criminal Division, Washington DC 20530-0001 or a National Archives and Records Administration (NARA) Regional Records Center.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Persons referred to in potential or actual cases and matters of concern to the Criminal Division and correspondence on subjects directed or referred to the Criminal Division.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system consists of alphabetical indices bearing individual names and the associated records to which they relate, arranged either by subject matter or individual identifying number containing the general and particular records of all Criminal Division correspondence, communications, matters and memoranda, including but not limited to, investigative reports, correspondence and from the Division, legal papers, evidence, and exhibits.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

This system is established and maintained pursuant to 44 U.S.C. 3101 to implement all functions assigned to the Criminal Division in 28 CFR 0.55 through 0.64–5. Additional authority is derived from Treaties, Statutes, Executive Orders, Presidential Proclamations, and Attorney General Directives.

PURPOSE(S):

Records in this system are used to provide investigative and litigation information to management in the Division and the Department, courts, and other law enforcement agencies.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

A record maintained in this system of records may be disseminated as a routine use of the record as follows:

(1) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

(2) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

(3) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

(4) To appropriate officials and employees of a federal agency or entity that requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

(5) A record may be disclosed to designated officers and employees of state, local, territorial law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy a position of public trust as a law enforcement officer or detention officer having contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.

(6) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(7) To an actual or potential party to litigation or administrative proceeding, or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.

(8) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(9) To federal, state, local, territorial, tribal, foreign (acting either directly or through an authorized representative of its government), or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

(10) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(11) To a former employee of the Department for purposes of: Responding to an official request by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(12) To such recipients and under such circumstances and procedures as are mandated

federal statute or treaty.

(13) To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation case arising from the matters of which they complained and/or of which they were a victim.

(14) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, tribal, or foreign (acting either directly or through an authorized representative of the government)), where the information is relevant to the recipient entity's law enforcement responsibilities.

(15) To a governmental entity lawfully engaged in collecting law enforcement, law enforcement intelligence, or national security intelligence information for such purposes.

(16) To any person, organization, or governmental entity in order to notify them of a serious terrorist threat for the purpose of guarding against or responding to such a threat.

(17) To any person or entity, or their representative, if deemed by the Criminal Division to be necessary in order to elicit information or cooperation from the person or entity or their representative for use by the Division in the performance of an authorized activity.

(18) A record that contains classified national security information and material may be disseminated to persons who are engaged in historical research projects, or who have previously occupied policy making positions to which they were appointed by the President in accordance with the provisions codified in 28 CFR 17.46.

(19) A record relating to an actual or potential civil or criminal violation of title 17, United States Code, may be disseminated to a person injured by such violation to assist him in the institution or maintenance of a suit brought under such title.

(20) A record relating to a person held in custody pending or during arraignment, trial, sentencing, or extradition proceedings, or after conviction or after extradition proceedings, may be disseminated to a federal, state, local, territorial, or foreign prison, probation, parole, pardon authority, or to any other agency or individual concerned with the maintenance, transportation, or release of such a person.

(21) A record relating to a case or matter that has been referred by an agency for investigation

prosecution or enforcement, or that involves a case or matter within the jurisdiction of an agency, may be disseminated to such agency to notify the agency of the status of the case or matter or of any decision or determination that has been made, or to make such inquiries or reports as are necessary during the processing of the case or matter.

(22) In any health care-related civil or criminal case, investigation, or matter, information indicating patient harm, neglect, or abuse, or poor or inadequate quality of care, at a health care facility or by a health care provider may be disclosed as a routine use to any federal, state, local, tribal, foreign, joint, international or private entity that is responsible for regulating, licensing, registering or accrediting any health care provider or health care facility, or enforcing any health care-related laws or regulations. Further, information indicating an ongoing quality of care problem by a health care provider or at a health care facility may be disclosed to an appropriate health plan. Additionally, unless otherwise prohibited by applicable law, information indicating patient harm, neglect, abuse, or poor or inadequate quality of care may be disclosed to the affected patient or his representative or guardian at the discretion of the manner determined by the agency in possession of the information.

(23) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft, fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are maintained in hard-copy, paper format and stored in electronic format via a

Storage Area Network system architecture consisting of personal computers, client/server and tape libraries. Data is stored on hard disk, floppy diskettes, compact disks, magnetic and/or optical disk media. Records are stored in accordance with applicable executive orders, statutes, and agency implementing regulations.

The computer storage devices are located at several Justice Department buildings in Washington, DC. Paper files are stored in: Division offices with controlled access; a security records unit with controlled access; locked file cabinets; other appropriate GSA approved security containers; or once closed, at a National Archives and Records Administration records center. Records that contain classified national security information are stored in accordance with applicable executive orders, statutes, and agency implementing regulations.

RETRIEVABILITY:

Records may be retrieved by reference to an individual's name or personal identifier.

SAFEGUARDS:

Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including the Department's automated systems security and access policies. Records and technical equipment are maintained in a secured area with restricted access. The use of password protection identification features and other system protection methods restrict access. All physical access to the building(s) where this system of records is maintained is controlled and monitored by security personnel and accessed only by authorized Department personnel or by non-Department personnel properly authorized to assist in the conduct of an agency function related to these records.

RETENTION AND DISPOSAL:

Records in this system are retained and disposed of in accordance with records retention schedules approved by the National Archives and Records Administration (NARA) for the constituent system of records.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Attorney General, Criminal Division, U.S. Department of Justice, 950 Pennsylvania Avenue, NW., Washington DC 20530-0001.

NOTIFICATION PROCEDURE:

The major part of this system is exempted from this requirement under 5 U.S.C. 552a(j)(k)(1) or (k)(2). Inquiries should be addressed to: Chief, Freedom of Information Act/Privacy Unit, Criminal Division, Department of Justice, 950 Pennsylvania Avenue, NW., Washington DC 20530-0001.

RECORD ACCESS PROCEDURES:

Requests for access to a record in this system must be in writing and should be addressed to the Chief of the Freedom of Information Act/Privacy Act Unit noted above. The envelope letter should be clearly marked "Privacy Act Request". Requests must comply with the Department's regulations and be made in accordance with 28 CFR Part 16. They must include a general description of the records sought, the requester's full name, current address, date and place of birth, the name of the case or matter involved, if known, and the name of the judicial district involved, if known, or any other identifying number or information which may be of assistance in locating the record. Social Security numbers are not used by the Criminal Division for identification purposes and should not be provided. The request must be signed and dated and either notarized or submitted under penalty of perjury. Some information may be exempt from access provisions as described in the section entitled "Exemptions Claimed for the System." An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Record Access Procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment. Some information may be exempt from contesting record procedures as described in the section entitled "Exemptions Claimed for the System." An individual who is the subject of a record in this system may seek amendment of those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

RECORD SOURCE CATEGORIES:

Department officers and employees and other federal, state, local and foreign law enforcement and non-law enforcement agencies, corporations and businesses, private persons, with informants, and publicly available information, including commercial information reseller

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3), (c)(4), (d), (e)(e)(2), (e)(3), (e)(4) (G), (H) and (I), (e)(5), (e)(8), (f) and (g) of the Privacy Act pursuant provisions of 5 U.S.C. 552a(j)(2); in addition, the system is exempt pursuant to the provisions of 5 U.S.C. 552a(k)(1) and (k)(2) from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (e) and have been published in the *Federal Register*. See 28 CFR 16.91.

[\[TOP\]](#)

JUSTICE/CRM-002

System name:

Criminal Division Witness Security File.

System location:

U.S. Department of Justice, Criminal Division, 10th Street and Constitution Avenue, NW Washington, DC 20530. In addition, some of the records contained in this system may be located at one or more of the Organized Crime and Racketeering Sections Field Offices in the appendix to the Criminal Division Systems of Records.

Categories of individuals covered by the system:

Persons who are potential or actual witnesses and/or informants, relatives, and associates of those individuals.

Categories of records in the system:

The system consists of the Witness Security Program files on all persons who are considered for admission or who have been admitted into the program. The files contain information

concerning the individuals, the source and degree of danger to which they are exposed cases in which they are expected to testify, relocation information and documentation, job assistance, sponsoring office, requirements for reimbursement and administration of the program, and protection techniques. Records concerning subject matters described in this system may also be contained in JUSTICE/CRM-001.

Authority for maintenance of the system:

This system is authorized pursuant to sections 501 through 504 of Pub. L. 91-452.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of a record as follows: 1. Dissemination of a record may be made to a federal, state, local, or foreign agency to acquire information concerning the individual, or those associated with the individual, relating to the protection of the subject or to a criminal investigation; 2. in any case in which there is an indication of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, the record in question may be disseminated to the appropriate federal, state, local, or foreign agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law; 3. in the course of investigating the potential or actual violation of any law, whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing of such violation, a record may be disseminated to a federal, state, local, or foreign agency, or to an individual or organization if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant; 4. a record relating to a case or matter may be disseminated to an appropriate federal, state, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practice; 5. a record relating to a case or matter may be disseminated to a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing; 6. a record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining, or informal discovery proceedings; 7. a record relating to an individual in a matter that has been referred for either consideration or investigation to an agency may be disseminated to the referring agency to notify such agency of the status

case or matter or of any decision or determination that has been made; 8. a record relating to an individual held in custody pending arraignment, trial, or sentence, or extradition proceedings, or after conviction or after extradition proceedings, may be disseminated to a federal, state, local, or foreign prison, probation, parole, or pardon authority, or to any other agency or individual concerned with the maintenance, transportation, or release of such person; 9. a record may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States or to an executive agreement; 10. a record may be disseminated to a federal, state, local, or foreign law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency; 11. a record may be disseminated to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter; 12. a record may be disseminated to a non-governmental entity or individual in the acquisition of employment or other services in behalf of the witnesses.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA), and the General Services Administration (GSA): A record from a system of records may be disclosed for a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional.

licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

A record contained in this system is kept on index cards and in files stored in safe type cabinets.

Retrievability:

A record is retrieved by name of the individual.

Safeguards:

The records are maintained in safes with additional physical safeguards as well as limited access by Departmental personnel.

Retention and disposal:

Currently there are no provisions for the disposal of the records in the system.

System manager(s) and address:

Assistant Attorney General; Criminal Division; U.S. Department of Justice; 10th Street and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Inquiry concerning the system should be addressed to the System Manager listed above.

Record access procedures:

The major part of this system is exempted from this requirement under 5 U.S.C. 552a(j)

(k)(1), or (k)(2). To the extent that this system of records is not subject to exemption, it is subject to access and contest. A determination as to exemption shall be made at the time request for access is received. A request for access to a record contained in this system must be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." Include in the request the name of the individual involved, his birth date and place, or another identifying number or information which may be of assistance in locating the record, the name of the case or matter involved, if known, and the name of the judicial district involved, if known. The requestor will also provide a return address for transmitting the information. All requests will be directed to the system manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the system manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

1. Federal, state, local, or foreign government agencies concerned with the administration of criminal justice; 2. Members of the public; 3. Government agency employees; 4. Published material; 5. Persons considered for admission or admitted to the program.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(4)(G), (H) and (I), (e)(5) and (8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/CRM-003

System name:

File of Names Checked to Determine If Those Individuals Have Been the Subject of An

Electronic Surveillance.

System location:

U.S. Department of Justice; Criminal Division; Bond Building, 1400 New York Avenue N
Washington, DC 20530.

Categories of individuals covered by the system:

Grand jury witnesses, defendants and potential defendants in criminal cases and their attorneys.

Categories of records in the system:

The system contains the names of those persons submitted by federal prosecutors to inquire whether such persons have been the subject of electronic surveillances. The file consists of the names, the inquiries made to federal investigatory agencies, the replies received from the agencies, and the reply submitted to the prosecutor. Records concerning subject matter described in this system may also be contained in JUSTICE/CRM-001.

Authority for maintenance of the system:

This system is established and maintained pursuant to 44 U.S.C. 3101. The system is also maintained to implement the provisions of 18 U.S.C. 3504.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of the record as follows: 1. In the appropriate federal court proceeding in accordance with established constitutional, substantive, or procedural law or practice; 2. to an actual or potential party or attorney in the case or matter in which the request was made.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion

personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject to the record.

Release of information to the National Archives and Records Administration (NARA), and the General Services Administration (GSA): A record from a system of records may be disclosed for a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

A record contained in this system is stored manually in file jackets.

Retrievability:

A record is retrieved by the name of the individual checked.

Safeguards:

The records are safeguarded and protected in accordance with applicable Departmental policies and procedures.

Retention and disposal:

Currently, there are no provisions for disposal of the records in this system.

System manager(s) and address:

Assistant Attorney General, Criminal Division, U.S. Department of Justice, 10th and Constitution Avenue NW, Washington, DC 20530.

Notification procedure:

A part of this system is exempted from this requirement under 5 U.S.C. 552a(j)(2). Inquiries concerning this system should be directed to the System Manager listed above.

Record access procedures:

A part of this system is exempted from this requirement under 5 U.S.C. 552a(j)(2). To the extent that this system of records is not subject to exemption, it is subject to access and contest. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record from this system shall be made in writing, with an envelope and the letter clearly marked "Private Access Request." Include in the request the name of the individual involved, his birth date and place, or any other identifying number or information which may be of assistance in locating the record, the name of the case or matter, if known, and the name of the judicial district involved, if known. The requestor will also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in this system are an actual or potential party or his attorney in the case or matter in question, federal prosecutors, and the federal investigative agency.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(4), (d), (e)(4) (G), and (I), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/CRM-006

System name:

Information File on Individuals and Commercial Entities Known or Suspected of Being Involved in Fraudulent Activities.

System location: U.S. Department of Justice, Criminal Division, 10th Street and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system: Individuals involved in actual or suspected fraudulent activities and their victims.

Categories of records in the system: This system of records consists of alphabetized indices of the names of those individuals or commercial entities known or suspected of involvement in fraudulent activities both foreign and domestic, and of computerized printouts of information obtained from documents, records, and other files in the possession of the Criminal Division that indicate the scope, details, and methods of operation of known or suspected fraudulent activities. The system also consists of documents, records, and other files to which the printouts relate. Records concerning subject matters described in this system may also be contained in CRM- 001.

Authority for maintenance of the system: This system is established and maintained pursuant to 44 U.S.C. 3101, and is intended to assist in implementing and enforcing criminal laws of the United States, codified in title 18, United States Code and elsewhere, particularly the laws relating to offenses involving fraudulent activities. The system is maintained to implement the provisions codified in 28 CFR 0.55, particularly subsection

Routine uses of records maintained in the system, including categories of users and purposes of such uses: A record maintained in this system of records may be disseminated as a routine use of such record as follows: (1) In any case in which there is an indication of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, a record in question may be disseminated to the appropriate federal, state, local, or foreign agency charged with the responsibility for investigating or prosecuting such violation or to an agency charged with enforcing or implementing such law; (2) in the course of investigating a potential or actual violation of any law, whether civil, criminal, or regulatory in nature, during the course of a trial or hearing or the preparation for a trial or hearing for such violation, a record may be disseminated to a federal, state, local, or foreign agency, individual or organization, if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, trial, or hearing and such dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant; (3) a record relating to a case or matter may be disseminated in an appropriate federal, state, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural practice; (4) a record relating to a case or matter may be disseminated to a federal, state, local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing; (5) a record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation, discussion on such matters as settlement of the case or matter, plea bargaining, or discovery proceedings; (6) a record relating to a case or matter that has been referred to an agency for investigation, prosecution, or enforcement, or that involves a case or matter within the jurisdiction of an agency, may be disseminated to such agency to notify the agency of the status of the case or matter or of any decision or determination that has been made, or to make such other inquiries and reports as are necessary during the processing of the case or matter; (7) a record relating to a person held in custody pending or during arraignment, trial, sentence, or extradition proceedings, or after conviction or after extradition proceedings, may be disseminated to a federal, state, local, or foreign probation, parole, or pardon authority, or to any other agency or individual concerned with the maintenance, transportation, or release of such a person; (8) a record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States or to an executive agreement; (9) a record may be disseminated to a federal, state, local, foreign, or international law enforcement agency to assist in the general crime prevention and detection efforts of such recipient agency or to provide investigative leads to such agency; (10) a record may be disseminated to a federal agency, in response to its request, in connection with the

or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter; (11) a record may be disseminated to the public, news media, trade associations, or organized groups, when the purpose of the dissemination is educational or informational, such as descriptions of crime trends distinctive or unique modus operandi, provided that the record does not contain any information identifiable to a specific individual other than such modus operandi; (12) a record may be disseminated to a foreign country, through the United States Department of State or directly to the representative of such country, to the extent necessary to assist such country in apprehending and/or returning a fugitive to a jurisdiction which seeks his

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage: A record contained in this system is stored on lists, index cards, and on carbon printout paper. The documents, records, and other files to which the printouts relate are stored in file jackets in file cabinets.

Retrievability: A record is retrieved by name of the individual, trade style used, or by any of the information of the preceding.

Safeguards: The computer center is maintained by the Office of Management and Financial Affairs, which has designed security procedures consistent with the sensitivity of the data. Materials related to the system maintained at locations other than the location of the computer center are protected and safeguarded in accordance with applicable Department rules.

Retention and disposal: Currently there are no provisions for disposal of records contained in this system.

System manager(s) and address: Assistant Attorney General, Criminal Division, U.S. Department of Justice, 10th Street and Constitution Avenue, NW, Washington, DC 20530

Notification procedure: Inquiries concerning the system should be directed to the System Manager listed above.

Record access procedures: The major part of this system is exempted from this requirement under 5 U.S.C. 552a (j)(2), (k)(1), or (k)(2). To the extent that this system of records is subject to exemption, it is subject to access and contest. A determination as to whether a request shall be made at the time a request for access is received. A request for access to a record contained in this system shall be made in writing, with the envelope and the letter clearly marked 'Privacy Access Request'. Include in the request the name of the individual involved, his birth date and place, or any other identifying number or information which may be of assistance in locating the record, the name of the case or matter involved, if known, and the name of the judicial district involved, if known. The requestor will also provide a return address for transmitting the information. Access requests will be directed to the system manager listed above. Records in this system are exempt from the access provisions of the Act in accordance with the applicable exemption notice.

Contesting record procedures: *Individuals desiring to contest or amend information maintained in the system should direct their request to the system manager listed at the top of the record, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Records in the system are exempt from the contesting provisions of the Act in accordance with the applicable exemption notice.*

Record source categories: *Federal, state, local, or foreign agencies, investigators, attorneys, prosecutors, private organizations, quasi-governmental agencies, trade associations, individuals, publications, and the news media.*

Systems exempted from certain provisions of the act: *The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(1), (2), and (3), (e)(4)(G), (H) and (I), and (8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the Federal Register.*

[\[TOP\]](#)

JUSTICE/CRM-008

System name:

Name Card File on Department of Justice Personnel Authorized to Have Access to Classified Files of the Department of Justice.

System location:

U.S. Department of Justice, Criminal Division, 10th and Constitution Avenue NW, Washington, DC 20530.

Categories of individuals covered by the system:

Current personnel of the Department of Justice, generally attorneys.

Categories of records in the system:

This index file contains the names of those attorneys and others currently employed in the Department of Justice who are authorized to have access to records of the Department of Justice classified in the interest of national security with such designations as confidential, secret, and top secret.

Authority for maintenance of the system:

This system is established pursuant to Executive Order No. 11652. The system is also maintained to implement the provisions codified in 28 CFR 17.1 through 17.82.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

There are no uses of the records in this system outside of the Department of Justice.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA), and the General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating

communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

A record contained in this system is stored manually on index cards.

Retrievability:

A record is retrieved by name from the index cards.

Safeguards:

The index is contained in the vault maintained for classified files of the Department of Justice.

Retention and disposal:

The names in the index are maintained and deleted in accordance with Departmental regulations.

System manager(s) and address:

Assistant Attorney General, Criminal Division, U.S. Department of Justice, 10th Street and Constitution Avenue NW, Washington, DC 20530.

Notification procedure:

Same as the above.

Record access procedures:

A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request". Include in the request the name of the person making the request.

individual involved. The requestor will also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Personnel of the Department of Justice.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/CRM-012

System name:

Organized Crime and Racketeering Section, General Index File and Associated Records

System location:

U.S. Department of Justice, Criminal Division, Organized Crime and Racketeering Section
Street and Constitution Avenue NW, Washington, DC 20530.

Categories of individuals covered by the system:

Persons who have been prosecuted or are under investigation for potential or actual criminal prosecution as well as persons allegedly involved in organized criminal activity and those alleged to be associated with the subject.

Categories of records in the system:

The system consists of alphabetical indices bearing individual names and the associate records to which they relate, arranged either by subject matter or individual identifying number of all incoming correspondence, cases, matters, investigations, and memoranda assigned, referred, or of interest, to the Organized Crime and Racketeering Section. The records in this system concern matters primarily involving organized crime and include, but are not limited to: case files; investigative reports; intelligence reports; subpoena and grand jury files; records of warrants and electronic surveillances; records of indictment, prosecution, conviction, parole, probation, or immunity; legal papers; evidence; exhibits; items classified confidential, secret, and top secret; and various other files related to the Section's activities and its ongoing investigations, prosecutions, cases, and matters. Records concerning subject matters described in this system may also be contained in JUSTICE/CRM-001.

Authority for maintenance of the system:

This system is established and maintained pursuant to 44 U.S.C. 3101 and the Presidential Directive on the Federal Drive Against Organized Crime, issued May 5, 1966 (Weekly Compilation of Presidential Documents, Vol. 2, W. No. 18 (1966)). In addition, this system is maintained to assist in implementing and enforcing the criminal laws of the United States, particularly those codified in title 18, United States Code. This system is also maintained to implement the provisions codified in 28 CFR 0.55 particularly subsection (g).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of a record as follows: (1) In any case in which there is an indication of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, the record in question may be disseminated to the appropriate federal, state, local, or foreign agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law; (2) in the course of investigating the potential or actual violation of law, whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing for such violation, a record may be disseminated to a federal, state, local, or foreign agency, or to an individual, or organization, if there is reasonable belief that such agency, individual, or organization possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant; (3) a record relating

case or matter may be disseminated in an appropriate federal, state, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practice; (4) a record relating to a case or matter may be disseminated to a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing; (5) a record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining, or information discovery proceedings; (6) a record relating to a case or matter that has been referred to an agency for investigation, prosecution, or enforcement, or that involves a case or matter within the jurisdiction of an agency, may be disseminated to such agency to notify the agency of the status of the case or matter or of any decision or determination that has been made, or for such other inquiries and reports as are necessary during the processing of the case or matter; (7) a record relating to a person held in custody pending or during arraignment, trial, sentencing, or extradition proceedings, or after conviction or after extradition proceedings, may be disseminated to a federal, state, local, or foreign prison, probation, parole, or pardon authority or to any other agency or individual concerned with the maintenance, transportation, or care of such a person; (8) a record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States or to an executive agreement; (9) a record may be disseminated to a federal, state, local, foreign, or international law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency; (10) a record may be disseminated to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter; (11) a record may be disseminated to the public, news media, trade association, or organized groups, when the purpose of dissemination is educational or informational, such as descriptions of crime trends or distinctive or unique modus operandi, provided that the record does not contain information identifiable to a specific individual other than such modus operandi; (12) a record may be disseminated to a foreign country, through the United States Department of State or directly to the representative of such country, to the extent necessary to assist such country in apprehending and/or returning a fugitive to a jurisdiction which seeks his return; (13) a record that contains classified national security information and material may be disseminated to persons who are engaged in historical research projects, or who have previously occupied positions in policy making provisions to which they were appointed by the President, in accordance with the provisions codified in 28 CFR 17.60.

Information may be released to the news media and the public pursuant to 28 CFR 50.2 if it is determined that release of the specific information in the context of a particular case constitute an unwarranted invasion of personal privacy.

Information may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record; and a record may be released to the National Archives and Records Administration and to the General Services Administration in connection with management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Information relating to health care fraud may be disclosed to private health plans, or associations of private health plans, and health insurers, or associations of health insurers, for the following purposes: to promote the coordination of efforts to prevent, detect, investigate, and prosecute health care fraud; to assist efforts by victims of health care fraud to obtain restitution; to enable private health plans to participate in local, regional, and national health care fraud task force activities; and to assist tribunals having jurisdiction over claims against private health plans.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

The records in this system are stored on various documents, tapes, disc packs, and punch cards, some of which are contained in files, on index cards, or in related type materials.

Retrievability:

The system is accessed by name but may be grouped for the convenience of the user.

subject matter, e.g., parole file, photograph file, etc.

Safeguards:

Materials related to the system are maintained in appropriately restricted areas and are safeguarded and protected in accordance with applicable Department rules.

Retention and disposal:

Currently there are no provisions for the disposal of the records in the system.

System manager(s) and address:

Assistant Attorney General, Criminal Division, U.S. Department of Justice, 10th Street and Constitution Avenue NW, Washington, DC 20530.

Notification procedure:

Inquiry concerning the system should be addressed to the System Manager listed above.

Record access procedures:

The major part of this system is exempted from this requirement under 5 U.S.C. 552a(j)(k)(1), or (k)(2). To the extent that this system of records is not subject to exemption, it is subject to access and contest. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record contained in this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." Include in the request the name of the individual involved, his birth date and place, or another identifying number or information which may be of assistance in locating the record, the name and of the case or matter involved, if known, and the name of the judicial district involved, if known. The requestor will also provide a return address for transmitting the information. Access requests will be directed to the system manager listed above. Records in this system are exempt from the access provisions of the Act in accordance with the appropriate exemption notice.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should di

their request to the system manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Records in this system are exempt from the contesting provisions of the Privacy Act in accordance with the applicable exemption notice.

Record source categories:

1. Federal, state, local, or foreign government agencies concerned with the administration of criminal justice and non-law enforcement agencies both public and private; 2. Members of the public; 3. Government employees; 4. Published material; 5. Witnesses and informants.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(3), (e)(4)(G), (H), and (I), (e)(5), and (8), (f), and (g) of the Privacy Act pursuant to U.S.C. 552a (j)(2). Rules have been promulgated in accordance with the requirements of U.S.C. 553(b), (c), and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/CRM-014

System name:

Organized Crime and Racketeering Section, Intelligence and Special Services Unit, Information Request System.

System location: U.S. Department of Justice, Criminal Division, 10th Street and Constitution Avenue, NW, Washington, DC 20530. In addition, some of the records contained in the system are located at one or more of the Organized Crime and Racketeering Section Offices listed in the appendix to the Criminal Division's systems of records.

Categories of individuals covered by the system: Individuals making inquiries of the Intelligence and Special Services Unit data sources, Unit personnel processing those inquiries, Intelligence Analysts assigned to the Strike Forces, and those individuals whom such inquiries are made.

Categories of records in the system: The information request record system provides

audit trail of the Organized Crime and Racketeering Section information system. Included in this system of records is such information as the request from an agency and the date of the request, the employee processing the request, the subject of the request, and a summary of the results of the check.

Authority for maintenance of the system: This system is established and maintained pursuant to 44 U.S.C. 3101. The system is also maintained to implement the provisions codified in 28 CFR 0.55 particularly subsection (g).

Routine uses of records maintained in the system, including categories of users and purposes of such uses: A record maintained in this system of records may be disseminated as a routine use of such record to a federal agency at its request if such agency has a need for the record to perform its duties.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance.

from the former employee regarding a matter within that person's former area of respon

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage: A record contained in this system is stored on computer tapes, paper, mag tape, and disc pack.

Retrievability: A record in this system is accessed by one or more of the component information contained in the system including accessing by the name of the individ

Safeguards: The computer center is maintained by the Office of Management and Fi which has designed security procedures consistent with the sensitivity of the data. Materials related to the system maintained at locations other than the location of the computer are similarly protected by being maintained in a restricted area at the Dep of Justice.

Retention and disposal: Information in the system is constantly modified as new information is received. Historical data is maintained as an audit trail until sufficient experience with the system is received to develop appropriate procedures for the elimination and destruction of the data. Such procedures are consistent with applic governmental procedures.

System manager(s) and address: Assistant Attorney General, Criminal Division, U.S Department of Justice, 10th Street and Constitution Avenue, NW, Washington, DC 2

Notification procedure: Inquiry concerning this system should be directed to the Sy Manager listed above.

Record access procedures: The major part of this system is exempted from this req under 5 U.S.C. 552a(j)(2), (k)(1), or (k)(2). To the extent that this system of records is subject to exemption, it is subject to access and contest. A determination as to exer shall be made at the time a request for access is received. A request for access to a contained in this system shall be made in writing, with the envelope and the letter c marked `Privacy Access Request`. Include in the request the name of the individual involved, his birth date and place, or any other identifying number or information w may be of assistance in locating the record, the name of the case or matter involved known, and the name of the judicial district involved, if known. The requestor will a

provide a return address for transmitting the information. Access requests will be directed to the system manager listed above. Records in this system are exempt from the access provisions of the Act in accordance with the applicable exemption notice.

Contesting record procedures: Individuals desiring to contest or amend information maintained in the system should direct their request to the system manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories: Individuals who make inquiry of the Organized Crime and Racketeering Information System.

Systems exempted from certain provisions of the act: The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(4)(G), (H) and (I), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the Federal Register.

[\[TOP\]](#)

JUSTICE/CRM-016

System name:

Records on Persons Who Have Outstanding and Uncollected Federal Criminal Fines or Federal Bond Forfeitures.

System location:

U.S. Department of Justice, Criminal Division, Bond Building, 1400 New York Avenue, N.W., Washington, DC 20530.

Categories of individuals covered by the system:

Persons who have outstanding and uncollected federal criminal fines or federal bond forfeitures whose address is presently unknown or was at one time, unknown.

Categories of records in the system:

This system contains the names of persons, and correspondence relating to such persons who have federal criminal fines or federal bond forfeitures outstanding and whose whereabouts are presently unknown or were, at one time, unknown. The system is maintained to gather information on the whereabouts of such persons and to assist in federal collection efforts.

Authority for maintenance of the system:

This system is established and maintained pursuant to 44 U.S.C. 3101. This system is maintained to implement the provisions codified in 28 CFR 0.171(a).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of a record as follows: (A) In the case of an individual whose whereabouts are unknown, to an individual organization, or government agency for the purpose of gathering information to locate such person; or (B) in the case of any individual whose name is contained in the system, whether or not his whereabouts are known as follows: (1) In any case in which there is an indication of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, the record in question may be disseminated to the appropriate federal, state, local, or foreign agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law; (2) in the course of investigating the potential or actual violation of any law, whether civil, criminal or regulatory in nature, or in the course of a trial or hearing or the preparation for a trial or hearing for such violation, the record may be disseminated to a federal state, local, or foreign agency, or to an individual organization if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or informant; (3) a record relating to a case or matter may be disseminated in an appropriate federal, state, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practices; (4) a record relating to a case or matter may be disseminated to a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing; (5) a record relating to a case or matter may be disseminated to an actual or potential party or attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining, or informal discovery proceedings; (6) a record may be

disseminated to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit to the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specified information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA), and the General Services Administration (GSA): A record from a system of records may be disclosed for routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

A record contained in this system is stored manually in file jackets.

Retrievability:

A record is retrieved by the name of the individual.

Safeguards:

Records are safeguarded and protected in accordance with applicable Department rule

Retention and disposal:

Currently there are no provisions for disposal of the records in this system.

System manager(s) and address:

Assistant Attorney General, Criminal Division, U.S. Department of Justice, 10th Street and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Same as the above.

Record access procedures:

A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked 'Privacy Access Request.' Include in the request the name and address of the individual involved, his address, his birth date and place, or other identifying number of information which may be of assistance in locating the record, the name of the individual involved, if known, and the name of the judicial district, if known. The requestor will also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

Individual desiring to contest or amend information maintained in the system should direct request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in this system are federal, state, local, or foreign agencies and private individuals and organizations.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/CRM-019

System name:

Requests to the Attorney General For Approval of Applications to Federal Judges For Electronic Interceptions.

System location:

U.S. Department of Justice, Criminal Division, 10th and Constitution Avenue, NW, Wash DC 20530.

Categories of individuals covered by the system:

Individuals who have been the subject of requests by federal investigative agencies for electronic surveillance.

Categories of records in the system:

The system contains requests received from federal investigative agencies and federal prosecutors, and associated documents, seeking the authorization of the Attorney General required by 18 U.S.C. 2516 for an application to a federal court for an order authorizing interception of a wire or oral communication in cases involving federal criminal violations. Records concerning subject matters described in this system may also be contained in JUSTICE/CRM-001.

Authority for maintenance of the system:

This system is established and maintained pursuant to 44 U.S.C. 3101. The system is maintained to implement the provisions of 18 U.S.C. 2516 and 18 U.S.C. 2519.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of the record as follows: 1. In an appropriate federal, state, or local court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practice; 2. to the requesting agency to notify such agency of the status of the case or matter or of any decision or determination that has been made; 3. to furnish such information for reports to the Administrative Office of the United States Courts as is necessary to comply with the reporting provisions of 18 U.S.C. 2519; 4. to a party pursuant to 18 U.S.C. 2518 (8)(d), (9), and (10); or 5. 18 U.S.C. 3504.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 18 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA), and the General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

A record contained in this system is stored manually in file jackets.

Retrievability:

A record is retrieved by the name of the individual who appears first on the application c affidavit that is first received.

Safeguards:

The records are safeguarded and protected in accordance with applicable Departmenta

Retention and disposal:

Currently there are no provisions for disposal of the records in this system.

System manager(s) and address:

Assistant Attorney General, Criminal Division, U.S. Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Inquiry concerning this system should be directed to the System Manager listed above.

Record access procedures:

The major part of this system is exempted from this requirement under 5 U.S.C. 552a (j)(k)(1), or (k)(2). To the extent that this system of records is not subject to exemption, it is subject to access and contest. A determination as to exemption shall be made at the time request for access is received. A request for access to a record contained in this system be made in writing, with the envelope and the letter clearly marked "Privacy Access Rec Include in the request the name of the individual involved, his birth date and place, or a other identifying number or information which may be of assistance in locating the recor name of the case or matter involved, if known, and the name of the judicial district invol known. The requestor will also provide a return address for transmitting the information.

requests will be directed to the system manager listed above. Records in this system are exempt from the access provisions of the Act in accordance with the applicable exemption notice.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the system manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Records in this system are exempt from the contesting provisions of the Act in accordance with the applicable exemption notice.

Record source categories:

Sources of information contained in this system are federal investigative agencies, federal prosecutors, and personnel of the Criminal Division, Department of Justice.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c) (3) and (4), (d), (e) and (3), (e)(4) (G), (H) and (I), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/CRM-021

System name:

The Stocks and Bonds Intelligence Control Card File System.

System location:

U.S. Department of Justice, Criminal Division, Bond Building, 1400 New York Avenue, N.W., Washington, DC 20530.

Categories of individuals covered by the system:

Individuals, and their known associates, who are actual, potential, or alleged violators, of the statutes dealing with stocks, bonds, and other securities.

Categories of records in the system:

This system is an alphabetical listing of all individuals, and their associates, who are actual, potential, or alleged violators of the statutes dealing with counterfeiting, forging, and the stocks, bonds, and other securities including those who traffic, or are suspected of trafficking in such stocks, bonds, or other securities. Records concerning subject matters described in this system may also be contained in JUSTICE/CRM-001.

Authority for maintenance of the system:

This system is established and maintained pursuant to 44 U.S.C. 3101, and is intended to assist in implementing and enforcing the criminal laws of the United States codified in the United States Code and elsewhere, particularly the laws relating to offenses involving stocks and bonds. The system is also maintained to implement the provisions codified in 28 C.F.R.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of the record as follows: (1) In any case in which there is an indication of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, the record in question may be disseminated to the appropriate federal, state, local, or foreign agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law; (2) in the course of investigating the potential or actual violation of law, whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing for such violation, a record may be disseminated to the federal, state, local, or foreign agency, or to an individual or organization, if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant; (3) a record relating to a case or matter may be disseminated in an appropriate federal, state, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural

law or practice; (4) a record relating to a case or matter may be disseminated to a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing; (5) a record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining, or information discovery proceedings; (6) a record relating to a case or matter that has been referred to an agency for investigation, prosecution, or enforcement, or that involves a case or matter within the jurisdiction of an agency, may be disseminated to such agency to notify the agency of the status of the case or matter or of any decision or determination that has been made, or in response to such other inquiries and reports as are necessary during the processing of the case or matter; (7) a record relating to a person held in custody pending or during arraignment, trial, sentencing, or extradition proceedings, or after conviction or after extradition proceedings, may be disseminated to a federal, state, local, or foreign prison, probation, parole, or pardon authority or to any other agency or individual concerned with the maintenance, transportation, or care of such a person; (8) a record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States or to an executive agreement; (9) a record may be disseminated to a federal, state, local, foreign, or international law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency; (10) a record may be disseminated to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter; (11) a record may be disseminated to the public, news media, trade associations, or organized groups, when the purpose of the dissemination is educational or informational, such as descriptions of crime trends or distinctive or unique modus operandi, provided that the record does not contain any information identifiable to a specific individual other than such modus operandi.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to

U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA), and General Services Administration (GSA): A record from a system of records may be disclosed for a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

A record contained in this system is stored manually on index cards.

Retrievability:

A record is retrieved by the name of the individual.

Safeguards:

Records are safeguarded and protected in accordance with applicable Departmental rules and regulations.

Retention and disposal:

Currently there are no provisions for disposal of the records in this system.

System manager(s) and address:

Assistant Attorney General, Criminal Division, U.S. Department of Justice, 10th Street and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Inquiry concerning the system should be directed to the System Manager listed above.

Record access procedures:

The major part of this system is exempted from this requirement under 5 U.S.C. 552a (j)(k)(1), or (k)(2). To the extent that this system of records is not subject to exemption, it is subject to access and contest. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record contained in this system must be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." Include in the request the name of the individual involved, his birth date and place, or any other identifying number or information which may be of assistance in locating the record, the name of the case or matter involved, if known, and the name of the judicial district involved, if known. The requester will also provide a return address for transmitting the information. All requests will be directed to the system manager listed above. Records in this system are exempt from the access provisions of the Act in accordance with the applicable exemption notice.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the system manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Records in this system are exempt from the contesting provisions of the Act in accordance with the applicable exemption notice.

Record source categories:

Sources of information contained in this system are federal, state, local, and foreign government agencies and prosecutors, private organizations and individuals, and persons within the Department of Justice.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(4)(G), (H) and (I), (e)(5) and (8), (f), and (g) of the Privacy Act pursuant to 552a (j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/CRM-022

System name:

Witness Immunity Records.

System location:

U.S. Department of Justice, Criminal Division, 10th Street and Constitution Avenue NW, Washington, DC 20530.

Categories of individuals covered by the system:

Potential or actual witnesses for whom immunity (pursuant to 18 U.S.C. 6001–6005) is proposed.

Categories of records in the system:

The system contains background information on the individual and the case of matter in which he is expected to testify in a proceeding before or ancillary to a court or grand jury of the United States or an agency of the United States. The information maintained in the system is from DOJ Form-LAA-111, "Request for Immunity Authorization", which is completed by United States Attorneys, or from other formal requests for immunity from Federal agencies. The system also contains a record of action taken by the Criminal Division on the request.

Authority for maintenance of the system:

This system is established and maintained pursuant to 44 U.S.C. 3101. The system is also maintained to implement the provisions of 18 U.S.C. 6001–6005 and 18 U.S.C. 2514.

Purpose(s):

The system is essential to the Division's efforts in granting immunity requests as stated U.S.C. 6001–6005. Requests for immunity may be made by a United States Attorney or Federal agency.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

(1) A record may be disseminated to a federal, state, local, or foreign law enforcement agency to alert such agency to the proposed immunity or, to the extent necessary for identification purposes, to elicit information concerning the potential or actual witness which may be necessary to an evaluation of the proposed immunity; (2) a record relating to a proposed immunity that has been referred to the Department of Justice for approval, may be disseminated to the referring agency to notify such agency of the status of the referral and decision or determination that has been made.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:***Storage:***

Paper documents are stored in file folders in locked cabinets; selected summary data are stored on magnetic disks and on manual index cards which are also kept in locked cabinets.

Retrievability:

Summary data, e.g., names, request numbers, dates of receipt and completion are retrieved from manual index cards for requests received prior to June 1986; for June 1986 and

subsequent years, summary data are retrieved from magnetic disks. File folders are accessed through the manual or automated indexes.

Safeguards:

The records are safeguarded and protected in accordance with applicable Departmental Security for the automated records include strictly controlled access codes and passwords. Only authorized Criminal Division employees will have access to the system.

Retention and disposal:

Dispose 10 years after close of request.

System manager(s) and address:

Assistant Attorney General, Criminal Division, U.S. Department of Justice, 10th Street and Constitution Avenue NW, Washington, DC 20530.

Notification procedure:

The major part of this system is exempted from this requirement pursuant to 5 U.S.C. 552(j)(2) or (k)(2). Inquiry concerning this system should be directed to the System Manager listed above.

Record access procedures:

The major part of this system is exempted from this requirement pursuant to 5 U.S.C. 552(j)(2) or (k)(2). To the extent that this system of records is not subject to exemption, it is available to access and contest. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record from this system shall be made in writing with the envelope and the letter clearly marked "Privacy Access Request". Include in the request the name of the individual involved, his birth date and place, or other identifying information which may be of assistance in locating the record, the name of the case or matter involved, if known, and the name of the judicial district involved, if known. The requester will also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring the contest or amend information maintained in the system should contact their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

1. Federal government prosecutors; 2. Federal agencies; 3. Department of Justice attorney and personnel.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c) (3) and (4), (d), (e) (3) and (e)(4) (G), (H) and (I), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552 (j)(2) and (k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/CRM-025

System name:

Tax Disclosure Index File and Associated Records.

System location:

U.S. Department of Justice, Criminal Division, Bond Building, 1400 New York Avenue N.W.
Washington, DC 20530.

Categories of individuals covered by the system:

Taxpayers about whom the Criminal Division has requested and/or obtained disclosure material from the Internal Revenue Service pursuant to 26 U.S.C. 6103.

Categories of records in the system:

The system contains all requests for tax material, any such material provided by the Internal Revenue Service or duplicated or extracted by the Criminal Division from such material, related records necessary to the application for and/or safeguarding of such material received on or after January 1, 1977.

Authority for maintenance of the system:

This system is established and maintained pursuant to 26 U.S.C. 6103(p)(4).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of : record (A) to any officer or employee of the Criminal Division who is personally and directly engaged in preparation for any proceeding (or investigation which may result in such proceeding) pertaining to the enforcement of a specifically designated Federal criminal statute not involving tax administration or to the enforcement of a Federal criminal statute in any manner involving tax administration; and (B) to any person outside of the Criminal Division when dissemination is or reasonably appears to be in furtherance of proper preparation for an proceeding (or investigation which may result in such proceeding) pertaining to the enforcement of a specifically designated Federal criminal statute not involving tax administration or to the enforcement of a Federal criminal statute in any manner involving tax administration. Such dissemination shall be permitted to the extent authorized under 26 U.S.C. 6103(h), 26 U.S.C. 6103(i), 26 CFR 404.6103(h)(2)–1, 26 CFR 404.6103(i)–(I), and Rule 61.1 of the Federal Rules of Criminal Procedure. The above mentioned routine uses include the following:

- (1) Dissemination to an attorney of the Criminal Division assigned responsibility with respect to an above-mentioned proceeding or an investigation which may result in such proceeding;
- (2) Dissemination to an officer or employee of the Department of Justice with supervisor or clerical responsibility with respect to an above-mentioned proceeding, or an investigation which may result in such proceeding;
- (3) Dissemination to an officer or employee of another Federal agency (as defined at 5 U.S.C. 551(1))

551(l)) with investigative, supervisory, or clerical responsibility working under the direct control of such attorneys of the Department of Justice as are assigned responsibility with respect to an above-mentioned proceeding, or an investigation which may result in such proceeding;

(4) Dissemination to a taxpayer to whom such record relates, or to such taxpayer's legal representative, to properly interview, consult, depose, or interrogate or otherwise obtain information relevant to an above-mentioned proceeding, or an investigation which may result in such proceeding, from such taxpayer or his legal representative;

(5) Dissemination during the course of an investigation which may result in an above-mentioned proceeding to any witness who may be called on to give evidence in such a proceeding to properly interview, consult, depose, or interrogate or otherwise obtain relevant information from such potential witness;

(6) Dissemination to any person having special knowledge or technical skills (such as handwriting analysis, photographic development, sound recording enhancement, or voice identification) to properly obtain the services of such person in an above-mentioned proceeding, or an investigation which may result in such proceeding;

(7) Dissemination to an officer or employee of the Department of Justice, another Federal agency (as defined at 5 U.S.C. 551(l)), or a foreign government to properly utilize intern contacts and judicial assistance in an above-mentioned proceeding, or an investigation which may result in such proceeding;

(8) Dissemination to an officer or employee of the Internal Revenue Service to obtain a disclosure pursuant to 26 U.S.C. 6103 in an above-mentioned proceeding, or an investigation which may result in such proceeding;

(9) Dissemination to a Federal grand jury;

(10) Dissemination to an officer or employee of the Department of Justice to obtain a court order to compel testimony pursuant to 18 U.S.C. 6002 and 6003 in any above-mentioned proceeding, or an investigation which may result in such proceeding;

(11) Dissemination to any party to an above-mentioned proceeding, to properly conduct

negotiations concerning, or obtain authorization for, disposition of the proceeding, in whole or in part, or to obtain stipulations of fact in connection with the proceeding;

(12) Dissemination to a judicial or administrative body (such as the United States Parole Commission) in an above-mentioned proceeding or in preparation therefore, or in any post-conviction proceeding resulting from an above-mentioned proceeding;

(13) Dissemination to a court reporter in an above-mentioned proceeding, or as required in preparation therefor.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

A record contained in this system is stored manually on index cards and in file jackets.

Retrievability:

A record is retrieved by name of the taxpayer in indices maintained in individual sections of the Criminal Division.

Safeguards:

Records are safeguarded in accordance with Department of Justice rules and procedures. Buildings in which records are located are under security guard, and access to premises requires official identification. Records are stored in spaces which are locked outside of normal office hours and in safe type filing cabinets which are locked when not being accessed. Access to such cabinets is limited to Division personnel whose duties and responsibilities require access.

access and to whom access may be permitted. A record of access is kept which indicates the name of each person who gains access to material from the secured area and the date and time of each access.

Retention and disposal:

Records not retained are returned to the Internal Revenue Service or rendered undisclosed in accordance with 26 U.S.C. 6103(p)(4)(f)(ii). Currently there are no provisions for disposal of records contained in this system that are not returned to the Internal Revenue Service or otherwise rendered undisclosable.

System manager(s) and address:

Assistant Attorney General, Criminal Division, U.S. Department of Justice, 10th Street and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

The major part of this system is exempted from this requirement under 5 U.S.C. 552a(j). Inquiry concerning the system should be addressed to the system manager listed above.

Record access procedures:

The major part of this system is exempted from this requirement under 5 U.S.C. 552a(j). To the extent that this system of records is not subject to exemption, it is subject to access contest. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record contained in this system shall be made in writing with the envelope and the letter clearly marked 'Privacy Access Request.' Include in the request the name of the individual involved, his birth date and place or any other identifying number or information which may be of assistance in locating the record, the name of the case or matter involved, if known, and the name of the judicial district involved, if known. The requestor will also provide a return address for transmitting the information. Access requests will be directed to the system manager listed above. Records in this system are exempt from the access provisions of the Act in accordance with the applicable exemption notice.

Contesting record procedures:

Taxpayers desiring to contest or amend information maintained in the system should direct

their request to the system manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Records in this system are exempt from the contesting provisions of the Privacy Act in accordance with the applicable exemption notice.

Record source categories:

Sources of information contained in this system are the Internal Revenue Service, Federal Bureau of Investigation, Federal investigative agencies, Federal prosecutors, and personnel of the Criminal Division, Department of Justice.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c) (3) and (4), (d), (e) (2) and (3), (e)(4)(G), and (H) and (I), (e) (5) and (8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/CRM—026

System name:

International Prisoner Transfer Case Files/International Prisoner Transfer Tracking System

System location:

U.S. Department of Justice, Criminal Division, Office of Enforcement Operations, 950 Pennsylvania Ave., NW., Washington, DC 20530.

Categories of individuals covered by the system:

Prisoners transferred to or from prisons in the United States under international prisoner transfer treaties between the United States and foreign nations. Please note that prisoners being transferred from prisons in the United States pursuant to international prisoner transfer treaties are primarily foreign nationals who are generally not protected by the Privacy Act.

rare cases, such individuals may hold dual citizenship or may be lawful permanent residents of the United States. Accordingly, the purpose of this notice is to cover only United States Citizens and lawful permanent residents who are included in this information system.

Categories of records in the system:

Paper Files: The system contains the individual case files of prisoners who have applied to be granted transfers to serve the balance of their sentences in their native countries. The system includes both United States citizens who have applied to return to the United States and foreign nationals who have applied to be transferred to foreign countries. The system may include, but is not limited to, the following information: The application for transfer; investigatory material; court-related documents; prison progress reports; media reports; and other correspondence; and interagency and intra-agency reports and recommendations and decisional documents relating to individual transfer matters.

Computerized Records: The system also includes an automated database for tracking the handling of prisoner transfer cases from application to final action. Information used to track such progress may include, but is not limited to, the prisoner's name, social security number, birth date, place of birth, offenses and sentencing information and other case-related information.

Authority for maintenance of the system:

The system is maintained to implement the provisions of 18 U.S.C. 4100 et. seq. The records maintained in the system are used to evaluate international prisoner transfer applications, to determine whether a particular application should be granted or denied, to respond to inquiries regarding transfer applications and determinations, to respond to subsequent litigation regarding prisoner transfer determinations and/or the validity of prisoner consent, and to permit periodic reports to Congress and others on matters relating to international prisoner transfers.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records, or information derived therefrom, in this system of records may be disclosed to the following:

(a) In appropriate proceedings before a court, grand jury, or administrative or regulatory

when records are determined by the Department of Justice, or the adjudicator, to be arg relevant to the proceeding.

(b) A State, territorial, local or foreign government, at its request, when the record relate one of its past or present prisoners.

(c) Such recipients and under such circumstances and procedures as are authorized by Federal statute or treaty.

(d) An appropriate Federal, State, territorial, local, foreign, or tribal law enforcement aut other appropriate agency charged with the responsibility for investigating or prosecuting violation or potential violation of law (whether civil, criminal, or regulatory in nature).

(e) A Federal, State, territorial, local, foreign or tribal agency, including prosecution, corrections, sentencing, or parole authorities, in order to assist in the execution of appr actions necessary to implement an international prisoner transfer decision, or in the performance of its official duties.

(f) Any Federal government agency for all purposes relating to the monitoring and contr entry of individuals into the United States.

(g) The news media and the public pursuant to 28 CFR 50.2, unless it is determined th release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(h) A Member of Congress or staff acting upon the Member's behalf when the Member r requests the information on behalf of and at the request of the individual who is the sub the record.

(i) The National Archives and Records Administration and the General Services Adminis for records management inspections conducted under the authority of 44 U.S.C. 2904 a 2906.

(j) Current and former government employees, including law enforcement and judicial authorities, whose comments on a particular prisoner transfer matter are solicited by the International Prisoner Transfer Unit in connection with its investigation and review of suc

case, in order to enable such persons to formulate a response to the request.

(k) Contractors, grantees, experts, consultants, students and others performing or work a contract, service, grant cooperative agreement or other assignment for the Federal government, when necessary to accomplish an agency function related to this system c records.

(l) Former employees of the Department of Justice for purposes of responding to an offi inquiry by a Federal, State or local government entity or professional licensing authority accordance with applicable Department regulations; or facilitating communications with former employee that may be necessary for personnel-related or other official purposes the Department requires information and/or consultation assistance from the former em regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Electronic data is stored in electronic media via a configuration of client/server and pers computer. Computerized records are stored on hard disk, floppy diskettes, or compact c Paper records and electronic media recordings of prisoner transfer consent verification hearings are stored in individual file folders and file cabinets with controlled access, and other appropriate GSA approved security containers.

Retrievability:

Individual case files are retrieved by a file number assigned to each individual who appl or is granted a transfer. Information stored in the computerized case tracking system is retrieved primarily by searching under the name and/or Federal Bureau of Prisons' regis number, or other inmate number, assigned to the person who applied for or was grante transfer.

Safeguards:

Paper records are secured through the use of safes and/or restricted access to the spa which files are located. Electronic records are safeguarded in accordance with DOJ rule

policies governing automated systems security and access, including the maintenance of technical equipment in restricted areas and the required use of individual passwords and identification codes to access the system.

Retention and disposal:

Individual case files are stored in the International Prisoner Transfer Unit's work area while prisoner transfer request is pending, and generally for up to three years after the date of closing. Cases are closed upon completion of prisoner transfer, denial of transfer, or prior withdrawal of request to transfer. Thereafter, files are transferred to the Washington National Records Center in Suitland, Maryland or other designated records center. In accordance with Records Disposition Authority N1-60-93-16, all case files are retained for not less than three years after being closed. Thereafter, files may be destroyed, except that specific files, designated as significant because of widespread public interest, are transferred to the National Archives and Records Administration for permanent retention.

System manager(s) and address:

Assistant Attorney General, Criminal Division, FOIA/PA Unit, U.S. Department of Justice
Pennsylvania Avenue, NW., Washington, DC 20530.

Notification procedure:

Inquiry concerning this system should be in writing and made to the system manager listed above.

Record access procedures:

A request for access to a record contained in this system shall be made in writing to the system manager, with the envelope and letter clearly marked "Privacy Act Request." The request shall include the name of the individual involved, his birth date and place, or any other identifying number or information which may be of assistance in locating the record, and the name of the case or matter involved. The requester shall also provide a signature (which must be either notarized or submitted under penalty of perjury) and a return address for transmitting the information.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the system manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information.

Record source categories:

Court records, prisoner statements, and communications with other components and agencies of the United States and foreign governments.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/CRM-027

System name:

Office of Special Investigations (OSI) Displaced Persons Listings.

System location:

U.S. Department of Justice, Criminal Division, Bond Building, 1400 New York Avenue, N.W., Washington, DC 20530, and Federal Records Center, Suitland, Maryland 20409.

Categories of individuals covered by the system:

Individuals who applied for entry visas into the United States under the Displaced Persons Act in force from 1948 to 1952 and for whom the United States Army Counterintelligence Command assembled visa investigation files.

Categories of records in the system:

The system consists of alphabetical indexes bearing the names of persons who applied for entry visas under the Displaced Persons Acts, their visa applications, investigative reports,

any other supporting documents.

Authority for maintenance of the system:

This system is established and maintained pursuant to 44 U.S.C. 3101 and is intended assist in implementing and enforcing the criminal laws of the United States, particularly Criminal Statutes codified in "Criminal Laws," United States Code. The system is also maintained to implement the provisions codified in 28 CFR 0.55 and 0.61.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records are used by OSI personnel as source material to locate potential witness might be able to provide information of investigative interest. However, a record maintain this sytem of records may be disseminated as a routine use of such record as follows: (Records, or some part thereof, relating to a particular visa applicant, may become a par investigative record maintained in a published system of records entitled "Central Crimir Division Index File and Associated Records, JUSTICE/CRM-001" and be subject to the uses of that system; (2) a record relating to a case or matter may be disseminated to a l country pursuant to an international treaty or convention entered into and ratified by the States or to an executive agreement; (3) a record may be disseminated to a Federal, St local, foreign, or international enforcement agency to assist in the general crime preven detection efforts of the recipient agency or to provide investigative leads to such agency (4) a record may be disseminated to a foreign country, through the United States Depart of State or directly to the representative of such country, to the extent necessary to assi country in apprehending and/or returning a fugitive to a jurisdiction which seeks his retu

Release of information to the news media:

Information permitted to be released to the news media and the public pursuant to 28 C 50.2 may be made available from systems of records maintained by the Department of , unless it is determined that release of the specific information in the context of a particu would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of re maintained by the Department of Justice, not otherwise required to be released pursuar U.S.C. 552, may be made available to a Member of Congress or staff acting upon the

Member's behalf when the Member or staff requests the information on behalf of and at request of the individual who is the subject of the record.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Index records in this system will be stored by name and control number on an IBM System 360. The actual records are papers in files stored in file boxes on shelves in locked record storage rooms.

Retrievability:

Records stored in this system can be retrieved by the name of the individual, and by the control number of the record.

Safeguards:

Appropriate steps have been taken to preserve security and minimize the risk of unauthorized access to the system. Staff members who use the computer to input data or who have access to the stored data have been given specific identification codes or passwords by the system security officer which will restrict access to specific data. The files will be kept in a locked room with restricted access.

Retention and disposal:

Currently there are no provisions for the disposal of records in the system.

System manager(s) and address:

Assistant Attorney General, Criminal Division, U.S. Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Inquire in writing to the system manager listed above.

Record access procedures:

Portions of this system are exempt from disclosure and contest by 5 U.S.C. 552a(k)(2). all requests for access to those portions not so exempted by writing to the system manager identified above. Clearly mark the envelope and letter "Privacy Access Requests;" provide full name and notarized signature of the individual who is the subject of the record, his/ her date and place of birth, or any other identifying number or information which may assist in locating the record; and, a return address.

Contesting record procedures:

Direct all requests to contest or amend information maintained in the system to the system manager listed above. State clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information.

Record source categories:

The information in this system was originally compiled during the course of investigation undertaken by the United States Army Counter Intelligence Corps pursuant to the Displaced Persons Acts in effect from 1948 to 1952. For the most part, the information in this system was obtained directly from the visa applicant himself, but the records would also contain information from other individuals or entities which would have shed light on the information supplied by the visa applicant.

Systems exempted from certain provisions of the act:

The Attorney General has exempted certain categories of records in this system from subsection (d) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). Rules have been

promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e), and has been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/CRM-028

SYSTEM NAME:

Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence and Operations Center System.

SECURITY CLASSIFICATION:

Classified, sensitive.

SYSTEM LOCATION:

U.S. Department of Justice, 950 Pennsylvania Avenue NW., Washington, DC 20530-0000

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Individuals charged with, convicted of, or known, suspected, or alleged to be involved in illicit narcotic trafficking or other potentially related criminal activity, including but not limited to facilitating the transportation of narcotics proceeds, money laundering, firearms trafficking, alien smuggling, and terrorist activity, or involved with international organized crime. For purposes of this system, international organized crime refers to those self-perpetuating associations of individuals who operate internationally for the purpose of obtaining power, influence, money, and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence, or while protecting their illegal activities through an international organizational structure and the exploitation of international communication mechanisms. 2. Individuals with pertinent knowledge of some circumstance or aspect of a case or record subject, such as witnesses, associates of record subjects, informants, and law enforcement or intelligence personnel. 3. Individuals, reasonably suspected of engaging in money laundering, other financial crimes, terrorism, and other criminal activity, including individuals referenced in information provided to the Financial Crimes Enforcement Network from financial institutions and other sources. 4. Individuals

identified in or involved with the filing, evaluation, or investigation of reports under the B Secrecy Act and its implementing regulations. 5. Information about relevant immigrant and nonimmigrant visa applicants, including visa adjudication, issuance, and refusal information also collected.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records may contain investigative and intelligence information about the individuals in the system, including their identifying information such as, but not limited to, name, social security number, address, physical descriptions of appearance, license plate information, bank account number, location and activities, as well as other data which may assist the Organized Crime Drug Enforcement Task Force (OCDETF) Fusion Center in fulfilling its responsibilities and the International Organized Crime Intelligence and Operations Center (IOC-2) in fulfilling its responsibilities. Information includes multi-source data that may assist law enforcement agencies, regulatory agencies, and agencies of the U.S. foreign intelligence community and military community in executing their responsibilities with respect to drug trafficking, international organized crime, money laundering, firearms trafficking, alien smuggling, terrorism, and other enforcement efforts, including the identification, location, arrest and prosecution of suspects, and civil proceedings and other activities related to such enforcement activities. This system of records will not contain Federal tax returns and return information defined by 26 U.S.C. 6103.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Consolidated Appropriations Act, 2004, Public Law 108-199, 118 Stat. 3 (2004); Comprehensive Drug Abuse Prevention and Control Act of 1970, Public Law 91-513 (84 Stat. 1236); the Single Convention on Narcotic Drugs, 1961; the Organized Crime Control Act of 1970, Public Law 91-452 (84 Stat. 922); the Convention on Transnational Organized Crime, 2004; Executive Order 11396 (1968). Additional authority is derived from Treaties, Statutes, Executive Orders and Presidential Proclamations which the Department of Justice (DOJ) has been charged with administering.

PURPOSE(S):

This system of records will serve two primary purposes. The first purpose of this system of records is to facilitate the mission of the OCDETF Program, which is to reduce the drug problem by identifying, disrupting and dismantling the most significant international and domestic

supply and money laundering organizations and related criminal operations (e.g., arms traffickers, alien smugglers, terrorists). By establishing a central data warehouse for the compilation, fusion, storage, and comprehensive analysis of drug, financial, and related investigative information, OCDETF expects to produce a more complete picture of the activities of drug trafficking, money laundering, firearms trafficking, alien smuggling, terrorist, and criminal organizations and their memberships than any one such agency can produce by itself. Specifically, the OCDETF Fusion Center will develop investigative leads, operational intelligence products and strategic intelligence assessments on new or evolving threats. OCDETF Fusion Center intends to disseminate these analytical products, as appropriate, to Federal, state, local, tribal, territorial, and foreign law enforcement and regulatory agencies and to agencies of the U.S. foreign intelligence community and the military community, to assist them in enforcing criminal, civil, and regulatory laws related to drug trafficking, money laundering, firearms trafficking, alien smuggling, terrorism, and other crimes, including the identification, apprehension, and prosecution of individuals who threaten the United States national and international security and interests through their involvement in such crimes.

The second purpose of this system of records is to facilitate the mission of IOC-2 and its member agencies to significantly disrupt and dismantle those international criminal organizations posing the greatest threat to the United States. By establishing a central data warehouse for the compilation, fusion, storage, and comprehensive analysis of international organized crime, financial, and related investigative information, IOC-2 expects to produce a more complete picture of the activities of international criminal organizations and their memberships than any one such agency can produce by itself. Specifically, IOC-2 will develop investigative leads, operational intelligence products and strategic intelligence assessments on new or evolving threats. IOC-2 intends to disseminate these analytical products, as appropriate, to Federal, state, local, tribal, territorial, and foreign law enforcement and regulatory agencies and to agencies of the U.S. foreign intelligence community and the military community, to assist them in enforcing criminal, civil, and regulatory laws related to organized crime, terrorism, and other crimes, including the identification, apprehension, and prosecution of individuals who threaten the United States national and international security and interests through their involvement in such crimes.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Relevant information contained in this system of records may be disclosed as follows:

- (a) To any criminal, civil, or regulatory law enforcement authority (whether Federal, state, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.
- (b) To a governmental entity lawfully engaged in collecting law enforcement, law enforcement intelligence, or national security intelligence information for such purposes.
- (c) To any person or entity if deemed by the Department of Justice to be necessary in order to elicit information or cooperation from the recipient for use by the Department in the performance of an authorized law enforcement activity related to this system.
- (d) To the Department of State and components thereof to further the efforts of those agencies with respect to the national security and foreign affairs aspects of international drug trafficking, money laundering, firearms trafficking, alien smuggling, terrorism, and related crimes.
- (e) To the Department of Defense and components thereof to support its role in the detection and monitoring of the transportation of illegal drugs and money laundering in the United States or such other roles in support of counter-drug and money laundering law enforcement, counter-firearms trafficking, counter-alien smuggling, and related crimes as may be permitted by law.
- (f) To the United Nations and its employees to the extent that the information is relevant to the recipient's law enforcement or international security functions.
- (g) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
- (h) To the White House (the President, Vice-President, their staffs, and other entities of the Executive Office of the President), and, during Presidential transitions, to the President-elect and Vice-President Elect and for their designated transition team staff, for coordination of activities that relate to or have an effect upon the carrying out of the constitutional, statutory, and other official or ceremonial duties of the President, President-elect, Vice-President or Vice-President Elect.
- (i) To complainants and/or victims to the extent necessary to provide such persons with

information and explanations concerning the progress and/or results of the investigation case arising from the matters of which they complained and/or of which they were a victim.

(j) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(k) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

(l) To appropriate officials and employees of a Federal agency or entity that requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit.

(m) To designated officers and employees of state, local, territorial, or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.

(n) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system's records.

(o) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(p) To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

(q) To the National Archives and Records Administration in records management inspection conducted under the authority of 44 U.S.C. 2904 and 2906.

(r) To a former employee of the Department for purposes of: responding to an official inquiry from a Federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(s) To appropriate agencies, entities, and persons when (1) it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(t) To Federal, state, local, territorial, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

(u) To any person, organization, or governmental entity in order to notify them of a serious terrorist threat for the purpose of guarding against or responding to such a threat.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Computerized records are stored on hard disk or removable storage devices. Some

information, including investigative files and information incorporated into analytical products may be retained in hard copy format and stored in individual file folders and file cabinet controlled access, and/or other appropriate GSA-approved security containers.

RETRIEVABILITY:

Access to individual records is gained by use of data retrieval capabilities of computers acquired and developed for processing of information in the OCDETF Fusion Center and IOC-2 System. Data will be retrieved through a number of criteria, including personal identifying information such as name and social security number.

SAFEGUARDS:

These records are housed in a secure building restricted to DOJ employees and other authorized personnel, and those persons transacting business with the DOJ who are escorted by DOJ or other authorized personnel. Physical and electronic access to the System is safeguarded in accordance with DOJ rules and policies governing automated systems and access, including the maintenance of technical equipment in restricted areas. The selection of containers or facilities is made in consideration of the sensitivity or National Security Classification as appropriate, of the files. The System is contained in a room secured by intruder alarms and other appropriate physical and electronic security controls. Access to the System terminal(s) are further restricted to DOJ employees, detailees to DOJ from other government agencies, and individual contractors who have authorized access (including individual passwords and identification codes), appropriate security clearances, and a demonstrated and lawful need to know the information in order to perform assigned functions on behalf of the OCDETF Fusion Center and/or IOC-2. All OCDETF Fusion Center and personnel capable of accessing the OCDETF Fusion Center and IOC-2 System will have successfully passed a background investigation. Unauthorized access to the telecommunications terminals is precluded by a complex authentication procedure.

RETENTION AND DISPOSAL:

Records in this system are maintained and disposed of in accordance with appropriate authority of the National Archives and Records Administration.

SYSTEM MANAGER AND ADDRESS:

Director, Executive Office for the Organized Crime Drug Enforcement Task Force, Criminal

Division, U.S. Department of Justice, 950 Pennsylvania Avenue NW., Washington, DC 20530-0001.

NOTIFICATION PROCEDURE:

Inquires should be addressed to: OCDETF Fusion Center Privacy Act/FOIA Unit, OCDETF Fusion Center, Executive Office for the Organized Crime Drug Enforcement Task Force Criminal Division, U.S. Department of Justice, 950 Pennsylvania Avenue NW., Washington, DC 20530-0001.

RECORD ACCESS PROCEDURES:

A request for access to a record from this system shall be made in writing to the System Manager, with the envelope and the letter clearly marked "Privacy Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. Some information may be exempt from access provisions as described in the section entitled "Exemptions Claimed for the System." An individual who is the subject of a record in this system may request those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their requests according to the Record Access Procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment, such as tax return information. Some information may be exempt from contesting record procedures described in the section entitled "Exemptions Claimed for the System." An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

RECORD SOURCE CATEGORIES:

Information provided by Federal, state, local, tribal, territorial, and foreign law enforcement

agencies; agencies of the U.S. foreign intelligence community and military community; and open sources, such as broadcast and print media and publicly-available data bases.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d)(1), and (4); (e)(1), (2), (3), (4)(G), (H) and (I), (5), and (8); (f); and (g) of the Privacy Act. The exemptions will be applied only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a (j) and/or (k). A determination as to exemption shall be made at the time a request for access or amendment is received. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and are published in today's *Federal Register*.

[\[TOP\]](#)

Drug Enforcement Administration

JUSTICE/DEA-001

System name:

Air Intelligence Program.

System location:

Drug Enforcement Administration, 1405 Eye Street, NW, Washington, DC 20537. Also, many field offices. See Appendix 1 for list of addresses.

Categories of individuals covered by the system:

(A) Aircraft Owners; (B) Licensed Pilots.

Categories of records in the system:

(A) FAA Civil Aircraft Registry; (B) FAA Aircraft Owners Registry; (C) FAA Airman Direct Entries into NADDIS.

Authority for maintenance of the system:

The System is maintained to provide intelligence and law enforcement activities pursuant to the Comprehensive Drug Abuse Prevention and Control Act of 1970 (Pub. L. 91-513) and Reorganization Plan No. 2 of 1973.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The system provides a research data base for identification of aircraft, aircraft owners and operators that are known or suspected of involvement in illicit air transportation of narcotics. Information developed from this system is provided to the following categories of users for law enforcement purposes on a routine basis: (A) Other Federal law enforcement agencies; (B) State and local law enforcement agencies; (C) Foreign law enforcement agencies with whom DEA maintains liaison.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the content of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or

official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Reference materials are maintained on microfiche. Information developed from the reference materials is entered onto the NADDIS magnetic tape.

Retrievability:

This system is indexed by name and identifying numbers.

Safeguards:

This system of records is maintained at DEA Headquarters which is protected by twenty-four hour guard service and electronic surveillance. Access to the building is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. Access to the system is restricted to authorized DEA employees with appropriate clearance on a need-to-know basis.

Retention and disposal:

Reference materials are retained until updated and then destroyed. Entries into NADDIS are retained for twenty-five years.

System manager(s) and address:

Deputy Assistant Administrator, Office of Intelligence, Drug Enforcement Administration
Eye Street, NW, Washington, DC 20537.

Notification procedure:

The reference materials in this system are matters of public record. Information developed by this system and entered into the Narcotics and Dangerous Drug Information System (NDDIS)

has been exempted from compliance with subsection (d) of the Act by the Attorney Gen

Record access procedures:

Same as above.

Contesting record procedures:

Same as the above.

Record source categories:

Federal Aviation Administration.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e and (3), (e)(4) (G), and (H), (e)(5) and (8), (f), (g), (h) of the Privacy Act pursuant to 5 U 552a (j) and (k). Rules have been promulgated in accordance with the requirements of U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DEA-003

System name:

Automated Records and Consolidated Orders System/Diversion Analysis and Detection (ARCOS/DADS).

Security classification:

Not Classified.

System location:

Drug Enforcement Administration, 700 Army Navy Drive, Arlington, VA 22202. Field office

identified on the DEA website at www.dea.gov.

Categories of individuals covered by the system:

Persons registered with the DEA under the Comprehensive Drug Abuse Prevention and Control Act of 1970. This includes any person who manufactures, manages, distributes, proposes to manufacture, manage, or distribute any controlled substance or List 1 chemical and every person who dispenses or proposes to dispense any controlled substance. These persons include licensed professionals such as doctors, dentists, pharmacists, or pharmaceutical manufacturers, as well as importers and chemical manufacturers.

Categories of records in the system:

The information contained in this system consists of documentation of individual business transactions between individuals who handle controlled substances at every level, from manufacturers down to ultimate consumers. Records include copies of controlled substance inventories, drug codes, deletion and adjustment reports, receipts, purchase orders, and prescriptions, and include the date of the transaction, the name, quantity, and quality of chemicals/substances purchased or dispensed, the parties to the transaction, and the DEA registrant numbers. This information provides an audit trail of all manufactured and/or imported controlled substances. Information can be retrieved from this system of records by using various data elements such as name, address, DEA registrant number, name of business, and social security number.

Authority for maintenance of the system:

This system of records is maintained pursuant to the reporting requirements of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 826(d)) and the United States treaty obligations under the Single Convention on Narcotic Drugs and Convention on Psychotropic Substances of 1971.

Purpose:

This system is used to track and report the transfer of pharmaceuticals and to detect pharmaceutical diversion.

Routine uses of records maintained in the system, including categories of users and

purposes of such uses:

Information contained in this system may be disclosed to the following categories of use the purposes stated:

A. Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, foreign, or tribal, law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.

B. To the International Narcotics Control Board as required by United States treaty obligations.

C. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

D. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record.

E. To the National Archives and Records Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

G. The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Disclosure to consumer reporting agencies:

Not applicable.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:***Storage:***

All automated data files associated with ARCOS/DADS are maintained in the Department of Justice Data Center and the Drug Enforcement Administration Data Center.

Retrievability:

Records on individuals are retrieved by name and DEA registration number.

Safeguards:

The portion of the records maintained in DEA headquarters is protected by twenty-four hour guard service and electronic surveillance. Access to all DEA facilities is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. Access to the system is restricted to DEA employees who have appropriate security clearances on a need to know basis. Access to automated records requires use of identification numbers which are issued to authorized DEA employees.

Retention and disposal:

Input data received from registrants is maintained for 60 days for backup purposes and then destroyed by shredding or electronic erasure. ARCOS master inventory records are retained for eight consecutive calendar quarters. As the end of a new quarter is reached, the oldest data is purged from the record. ARCOS transaction history will be retained for a maximum of five years and then destroyed.

System manager(s) and address:

Deputy Assistant Administrator, Office of Diversion Control, Drug Enforcement Administration, Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to Freedom of Information Section, Drug Enforcement Administration, Washington, DC 20537. Inquiries should include inquirer's name, date and social security number.

Record access procedures:

Same as the above.

Contesting record procedures:

Same as the above.

Record source categories:

Information is obtained from registrants under the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 826(d)).

Exemptions Claimed For the System:

The Attorney General has exempted this system from subsections (c)(3) and (d) of the Information Freedom Act pursuant to 5 U.S.C. 552a(k)(2). These exemptions are codified at 28 CFR 16.98. Regulations have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (d).

[\[TOP\]](#)

JUSTICE/DEA-005

System name:

Controlled Substances Act Registration Records (CSA).

System location:

Drug Enforcement Administration, 1405 Eye Street NW, Washington, DC 20537. Also, field offices. See Appendix 1 for list of addresses.

Categories of individuals covered by the system:

Records are maintained on the following categories of individuals registered under the Controlled Substances Act including registrants doing business under their individual name rather than a business name: (A) Physicians and related practitioners; (B) Dentists; (C) Veterinarians; (D) Persons conducting research with controlled substances; (E) Importers of controlled substances; (F) Exporters of controlled substances; (G) Manufacturers of controlled substances; (H) Distributors of controlled substances; (I) Pharmacies.

Categories of records in the system:

The Controlled Substances Act Registration Records are maintained in a manual system that contains the original of the application for registration under 224, 224a, 225, 225a, 226, 268, and 363a, order forms (DEA-222's) and any correspondence concerning a particular registrant. In addition, the same basic data is maintained in an automated system for quick retrieval.

Authority for maintenance of the system:

The Drug Enforcement Administration is required under the Comprehensive Drug Abuse Prevention and Control Act of 1970 (Pub. L. 91-513) to register all handlers of controlled substances.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The Controlled Substances Act Registration Records produce special reports as required for statistical analytical purposes. Disclosures of information from this system are made to the following categories of users for the purposes stated: (A) Other Federal law enforcement and regulatory agencies for law enforcement and regulatory purposes; (B) State and local law enforcement and regulatory agencies for law enforcement and regulatory purposes; (C) Persons registered under the Controlled Substances Act (Pub. L. 91-513) for the purpose of verifying the registration of customers and practitioners.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of

maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed for routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

The automated portion of this system is maintained on magnetic tape and the manual portion is by batch.

Retrievability:

The automated system is retrieved by name and registration number. The manual portion is filed in batches by date the application was processed. A microfiche system of the names of the States is maintained for quick reference purposes. In addition, a number of telecommunications terminals have been added to the existing network.

Safeguards:

This system of records is maintained in DEA Headquarters which is protected by twenty hour guard service and electronic surveillance. Access to the building is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. Access to the system is restricted to DEA personnel on a need-to-know basis. A specific computer program is necessary to extract information. Information that is retrieved by terminals requires user identification numbers which are issued to authorized employees of the Department of Justice.

Retention and disposal:

Records in the manual portion of the system are retired to the Federal Records Center for one year and destroyed after eight years. The automated data is stored in the Department of Justice Computer Center and destroyed after five years.

System manager(s) and address:

Deputy Assistant Administrator, Office of Diversion Control, Drug Enforcement Administration, 1405 Eye Street NW, Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to Freedom of Information Section, Drug Enforcement Administration, 1405 Eye Street NW, Washington, DC 20537. Inquiries should include inquirer's name, date of birth, and social security number.

Record access procedures:

Same as the above.

Contesting record procedures:

Same as the above.

Record source categories:

Information contained in this system of records is obtained from: (A) Registrants and ap under the Controlled Substances Act (Pub. L. 91–513); (B) DEA Investigators.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3), (d), (e)(4) (G) (H), (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b) (c), and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DEA–007

System name:

International Intelligence Data Base.

System location:

Drug Enforcement Administration, 1405 I Street NW, Washington, DC 20537. Also, field offices. See Appendix 1 for list of addresses.

Categories of individuals covered by the system:

Known and suspected drug traffickers.

Categories of records in the system:

(A) Intelligence reports; (B) Investigative reports; (C) Subject files.

Authority for maintenance of the system:

This system is maintained for law enforcement and intelligence purposes pursuant to the Comprehensive Drug Abuse Prevention and Control Act of 1970, Reorganization Plan Number 1 of 1973 and the Single Convention on Narcotic Drugs.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

This system is maintained to further criminal investigations through the collation, analysis and dissemination of intelligence information. This system produces the following reports: (a) Tactical, operational and strategic intelligence reports; (b) Major organizational reports; (c) Network analysis; (d) Trafficker profiles; (e) Intelligence briefs on prior experience with individuals, firms, countries, etc.; (f) Country profiles; (g) Country Intelligence Action Plans; (h) Current Situational reports; (i) Special reports as requested; (j) Drug patterns and trends in drug trafficking from source to U.S. distributors.

In addition, information is provided to the following categories of users for law enforcement purposes on a routine basis: (A) Other Federal law enforcement agencies; (B) State and local law enforcement agencies; (C) Foreign law enforcement agencies with whom DEA maintains liaison; (D) U.S. Intelligence and Military Intelligence Agencies involved in drug enforcement; (E) U.S. Department of State; (F) Committees and working groups under the Strategy on Drug Abuse.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of Information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of

in the system:***Storage:***

These records are maintained in standard case files and on index cards.

Retrievability:

The system is indexed by name and subject category and retrieved by use of a card file

Safeguards:

This system of records is maintained at DEA Headquarters which is protected by twenty hour guard service and electronic surveillance. Access to the building is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. In addition, all records contained in this system are stored in GSA approved security containers. Access to the System is restricted to authorized DEA personnel with Secret Clearance or above.

Retention and disposal:

The records contained in this system are currently retained for an indefinite period.

System manager(s) and address:

Assistant Administrator for Intelligence, Drug Enforcement Administration, 1405 I Street NW, Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to Freedom of Information Unit, Drug Enforcement Administration, 1405 I Street NW, Washington, DC 20537. Inquiries should include inquiry name, date of birth, and social security number.

Record access procedures:

Same as Notification Procedure.

Contesting record procedures:

Same as Notification Procedure.

Record source categories:

(A) Other Federal Agencies; (B) State and local law enforcement agencies; (C) Foreign enforcement agencies; (D) Confidential informants.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(4)(G), (H), (e)(5) and (8), (f), (g), and (h) of the Privacy Act pursuant to 5 U. 552a(j) and (k). Rules have been promulgated in accordance with the requirements of 5 553(b), (c), and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DEA-008

System name:

Investigative Reporting and Filing System, Justice/DEA-008.

System location:

Drug Enforcement Administration: 700 Army Navy Drive, Arlington, VA 22202; and field offices. For field office addresses, see appendix identified as "DEA Appendix—List of Record Location Addresses, Justice/DEA-999."

Categories of individuals covered by the system:

- A. Drug offenders
- B. Alleged drug offenders; and
- C. Persons suspected of drug offenses.

D. Defendants.

Such individuals may include individuals registered with DEA and responsible for the handling, dispensing, or manufacturing of controlled substances under the Comprehensive Drug Prevention and Control Act of 1970.

Categories of records in the system:

Subpart A:

Subpart A is (1) a manual index (which serves as a backup to the automated index described in subpart B) and (2) paper case file records consisting of: Criminal Investigative Files; Regulatory Audit and Investigatory Files; and General Investigative Files. These files may include investigative and confidential informant reports and all documented findings and investigative "lead" information relative to preregistrant inspections, investigations, target conspiracies, and trafficking situations, etc. The reports pertain to the full range of DEA criminal drug enforcement and regulatory investigative functions that emanate from the Comprehensive Drug Prevention and Control Act of 1970.

For example, records in the Criminal Investigative Case Files may include a systematic gathering of information targeted on an individual or group of individuals operating in illicit drugs either in the United States or internationally; reports on individuals suspected or convicted of narcotics violations; reports of arrests; information on drug possession, sale, or purchases by such individuals; and information on the transport of such drugs, either in the United States or internationally, by such individuals. Records in the Regulatory Audit and Investigatory Files may include similar investigative reports regarding those individuals specifically identified under item C. of the "Categories of Individuals Covered by the System." Records in the General Investigative Files may generally include fragmentary or low priority information on an individual which is not significant enough to open a case file.

Subpart B:

Subpart B is an automated index containing limited, summary-type data which are extracted from and which point to the case files maintained by DEA as described in subpart A and to files maintained by other Federal, State, or local law enforcement agencies. Example of such data include: Record number; subject name (person, business, vessel), aliases and

soundex; personal data; (occupation(s), race, sex, date and place of birth, height, weight, color, eye color, citizenship, nationality/ethnicity, alien status); special considerations (if armed/dangerous); resident and criminal address (business and personal); miscellaneous numbers (telephone, passport, drivers license, vehicles registration, social security number etc.); relevant case file numbers, with indicators for active investigations; date/stamp (event data). (Subpart B will contain no classified information.)

Authority for maintenance of the system:

This system is established and maintained to enable DEA to carry out its assigned law enforcement and criminal regulatory functions under the Comprehensive Drug Abuse Prevention and Control Act of 1970 (Pub. L. 91-513), Reorganization Plan No. 2 of 1973, Title 21 United States Code; and to fulfill United States obligations under the Single Convention on Narcotic Drugs.

Purpose(s):

The records in this system have been compiled for the purpose of identifying, apprehending and prosecuting individuals connected in any way with the illegal manufacture, distribution and use of drugs.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant records or any relevant facts derived therefrom may be disclosed to:

(1) Other Federal, State, local, and foreign law enforcement and regulatory agencies, and components thereof, to support their role in the detection and monitoring of the distribution of illegal drugs in the United States or such other roles in support of counterdrug law enforcement as may be permitted by law. Direct, electronic, "read only" access by Federal, State, or local law enforcement agencies only to subpart B of this system of records may be permitted to enable these agencies (i) to identify law enforcement information or activities that may be relevant to their law enforcement responsibilities and (ii) where such information or activities is identified, either request access from DEA to the underlying case file records described in subpart A or, where the case file is maintained by another agency, request from such other agency, and (iii) to ensure appropriate coordination of such activities with or other appropriate law enforcement agency. In addition, direct, electronic, read and write

access may be permitted, but only to the index data generated by the accessing agency; enable such agency to modify or delete its own data.

(2) Other Federal, State, local, and foreign law enforcement and regulatory agencies, a component thereof, to the extent necessary to elicit information pertinent to counter-drug enforcement;

(3) Foreign law enforcement agencies through the Department of State (with whom DEA maintains liaison), and agencies of the U.S. foreign intelligence community to further the efforts of those agencies with respect to the national security and foreign affairs aspects of international drug trafficking;

(4) Individuals and organizations in the course of investigations to the extent necessary to elicit information about suspected or known illegal drug violators;

(5) Federal and state regulatory agencies responsible for the licensing or certification of individuals in the fields of pharmacy and medicine to assist them in carrying out such licensing or certification functions;

(6) Any person or entity to the extent necessary to prevent an imminent or potential crime which directly threatens loss of life or serious bodily injury;

(7) news media and the public pursuant to 28 CFR 50.2 unless it is determined that Release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(8) A Member of Congress or staff acting upon the Member's behalf when the Member requests the information on behalf of and at the request of the individual who is the subject of the record;

(9) National Archives and Records Administration and the General Services Administration records management inspections conducted under the authority of 44 U.S.C. 2904 and 2905 and

(10) To a court or adjudicative body before which DEA is authorized to appear when any of the following is a party to litigation or has an interest in litigation and such records are determined to be relevant to the litigation.

by DEA to be arguably relevant to the litigation; (i) DEA, or any subdivision thereof, or (ii) any employee of DEA in his or her official capacity, or (iii) any employee of DEA in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (iv) the United States, where DEA determines that the litigation is likely to affect it or any subdivisions.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records described in subpart A of the "Categories of Records in the System" are maintained on standard index cards and in standard file folders at DEA Headquarters and field offices. Records described in subpart B are stored on a computer database at the DEA and on a mainframe at the Department of Justice Computer Center.

Retrievability:

Information will be retrieved by accessing either the manual or automated index by name or by cross-referencing the name with a number assigned to the case file. The law enforcement components of the Department of Justice may have direct, electronic, "read only" access to subpart B of the "Categories of Records in the System" (under subsection (b)(1) of the Privacy Act) to subpart B of the "Categories of Records in the System". These data will assist DOJ law enforcement components in identifying whether there may be detailed records which reside in subpart A of this system of records that may be relevant to their law enforcement responsibilities. Where such records are identified, DOJ law enforcement components may request access. In addition, DOJ law enforcement components may have direct, electronic "read and write" access to the index data generated by such components to modify or delete its own data.

Safeguards:

Access is limited to designated employees with a need-to-know. All records are stored in a secure area of a secure building. In addition to controlled access to the building, the area where records are kept are either attended by responsible DEA employees, guarded by a security guard, and/or protected by electronic surveillance and/or alarm systems, as appropriate. In addition, paper records, including the manual index, are in locked files during off-duty hours and unauthorized access to the automated index is also prevented through state-of-the-art technology such as encryption and multiple user ID's and passwords.

Retention and disposal:

Paper records will be transferred to the Washington National Records Center 10 years after date of last entry; and destroyed 25 years after date of last entry. The related index will be deleted 25 years after date of last entry. Approval pending DEA records management at NARA.

System manager(s) and address:

Assistant Administrator, Operations Division, Drug Enforcement Administration, Freedom of Information Section, Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to: Drug Enforcement Administration, Freedom of Information Section, Washington, DC 20537.

Record access procedure:

Same as above.

Contesting record procedure:

Same as above.

Record source categories:

(a) DEA personnel, (b) Confidential informants, witnesses and other cooperating individuals, (c) Suspects and defendants, (d) Federal, State and local law enforcement and regulatory agencies, (e) foreign law enforcement agencies, (f) business records by subpoena, and drug and chemical companies.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(5) and (8), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2). In addition, the system has been exempted from subsections (c)(3), (d), and (e)(1), pursuant to subsection (k)(1). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 5 (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DEA-009

System name:

Medical Records.

System location:

Drug Enforcement Administration; 1405 Eye Street NW, Washington, DC 20537. Also, field offices. See Appendix 1 for list of addresses.

Categories of individuals covered by the system:

(A) DEA employees; (B) Cooperating individuals;

Categories of records in the system:

(A) Annual physical examinations; (B) Reports of disease or injury pertaining to DEA Special Agents and Chemists; (C) Reports of job related injury or illness for employees and cooperating individuals; (D) Pre-employment physical examination of DEA Special Agent Investigators; (E) Physical examination reports of non-federal police personnel applying to attend the National Training Institute.

Authority for maintenance of the system:

These records are maintained to establish and maintain an effective and comprehensive program for employees pursuant to 5 U.S.C. 7901, 29 U.S.C. 655 and Executive Order of September 28, 1974.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records are maintained for internal DEA use. The only disclosure outside the agency would be to a physician when authorized by the subject.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from system of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personnel privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:***Storage:***

The records are maintained in standard file folders.

Retrievability:

Records are retrieved by name.

Safeguards:

This system of records is maintained at DEA Headquarters which is protected by twenty hour guard service and electronic surveillance. Access to the building is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. In addition, the records are stored in file safes in an alarmed, controlled access area. Access to the system is limited to employees of the medical office on a need-to-know basis.

Retention and disposal:

These records are retained indefinitely.

System manager(s) and address:

Medical Administration, Drug Enforcement Administration, 1405 Eye Street NW, Washington DC 20537.

Notification procedure:

Inquiries should be addressed to Freedom of Information Section, Drug Enforcement Administration, 1405 Eye Street NW, Washington, DC 20537. Inquiries should contain the following information: Name; Date and Place of Birth; Dates of Employment with DEA; Employee number.

Record access procedures:

Same as the above.

Contesting record procedures:

Same as above.

Record source categories:

Individuals on whom records are maintained; Employees of Medical Office.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/DEA-010

System name:

Planning and Inspection Division Records.

System location:

Drug Enforcement Administration, 1405 I Street, NW, Washington, DC 20537. Also, field offices. See Appendix I for list of addresses.

Categories of individuals covered by the system:

(A) DEA employees, past and present; (B) Applicants for employment with DEA; (C) Drug offenders, alleged drug offenders, and persons suspected of drug offenses; (D) Offenders, alleged offenders, and persons suspected of committing Federal and state crimes broadly characterized as corruption or integrity offenses; (E) Confidential informants; (F) Witnesses; (G) Nonimplicated persons with pertinent knowledge of circumstances or aspects with pertinent knowledge of circumstances or aspects of a case or suspect. These are pertinent references of fact developed by personal interview or third party interview and are recorded in a matter for which a probable need will exist.

Categories of records in the system:

(A) Investigative reports with supporting memoranda and work papers relating to investigation of individuals and situations. (B) General files which include, among other things, supporting memoranda and work papers and miscellaneous memoranda relating to investigations of

the purported existence of situations and allegations about individuals. (C) Audit and inspection reports of inspections of DEA offices, personnel, and situations.

Authority for maintenance of the system:

Reorganization Plan No. 1 of 1968 and 5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information contained in this system is provided to the following categories of users as a part of routine uses for law enforcement and regulatory purposes: A. Other Federal law enforcement and regulatory agencies; B. State and local law enforcement and regulatory agencies; C. Foreign law enforcement agencies with whom DEA maintains liaison; D. The Department of State; E. The Department of Defense and Military Departments; F. U.S. Intelligence agencies concerned with drug enforcement; G. The United Nations; H. International organizations; I. To individuals and organizations in the course of investigations to elicit information.

In addition, disclosures are routinely made to the following categories for the purposes stated: A. To Federal agencies for national security clearance purposes and to Federal and state regulatory agencies responsible for the licensing or certification of individuals in the fields of pharmacy and medicine; B. To the Office of Management and Budget upon request in order to justify the allocations of resources; C. To state and local prosecutors for assistance in preparing cases concerning criminal and regulatory matters; D. To the news media for public information purposes; E. To Federal, State and local governmental agencies who are conducting suitability for employment investigations on current or prospective employees.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the direction of the Member.

request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed in routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Manual records are maintained in standard investigation folders. Automated records are maintained on magnetic disks.

Retrievability:

Access to manual records can be accomplished by the use of a card index maintained alphabetically by employee name. Access to the automated system is achieved by reference to personal identifiers, other data elements or any combination thereof.

Safeguards:

These records are maintained at DEA Headquarters which is protected by twenty-four hour guard service and electronic surveillance. Access to the building is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. Access to the system is restricted to employees of the Office of Internal Security and upper level management officials. The records are stored in a vault protected by alarm and cipher locks. Access to the system will be on a strict need-to-know basis.

Retention and disposal:

Case files are destroyed after five years unless the Office of Internal Security of the Chief Counsel determines that these files are required for potential or ongoing litigation. This determination will be subject to annual review. General files and audit files shall be retained as long as the subject is employed at DEA and for two years after termination.

System manager(s) and address:

Security Programs Manager, Drug Enforcement Administration, 1405 I Street NW, Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to Freedom of Information Section, Drug Enforcement Administration, 1405 I Street NW, Washington, DC 20537.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

(A) DEA Investigations; (B) Federal, State and local law enforcement agencies; (C) Cooperating individuals.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c), (3) and (4), (d), (2) and (3), (e)(4) (G), (H) (e) (5) and (8), (f), (g), (h) of the Privacy Act pursuant to 5 U.S.C. 552a (j) and (k). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DEA-011

System name:

Operations Files.

System Location:

Drug Enforcement Administration, 1405 Eye Street, NW, Washington, DC 20537. Also, 1 offices. See Appendix 1 for list of addresses.

Categories of individuals covered by the system:

(A) Cooperating Individuals; (B) Confidential Informants.

Categories of records in the system:

(A) Biographic and background information; (B) Official Contact Reports; (C) Intelligence Reports (DEA-6).

Authority for maintenance of the system:

This system of records is maintained to assist in intelligence operations pursuant to the Comprehensive Drug Abuse Prevention and Control Act of 1970 (Pub. L. 91-513) and Reorganization Plan No. 2 of 1973.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

This system is used to keep a history of intelligence operations against narcotics traffickers and their support networks. Information contained in this system is provided to the following categories of users for law enforcement purposes on a routine basis: (A) Other Federal law enforcement agencies; (B) State and local law enforcement agencies; (C) Foreign law enforcement agencies with whom DEA maintains liaison; (D) United States Intelligence Community Military Intelligence agencies involved in drug enforcement; (E) The United States Department of Justice.

of State.

Release of information to the news media. Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed for a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

These records are maintained in standard case files.

Retrievability:

These files are retrieved manually by subject matter category and coded identification number.

Safeguards:

This system of records is maintained at DEA Headquarters which is protected by twenty hour guard service and electronic surveillance. Access to the building is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. In addition, all files are stored in GSA approved security containers appropriate for Secret material and treated as if they carried a Secret classification whether classified or not. Access to the files is restricted to authorized DEA employees with Top Secret clearance on a limited need-to-know basis.

Retention and disposal:

These records are retained indefinitely.

System manager(s) and address:

Deputy Assistant Administrator, Office of Intelligence, Drug Enforcement Administration
Eye Street NW, Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to Freedom of Information Section, Drug Enforcement Administration, 1405 I Street NW, Washington, DC 20537.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

(A) DEA Reports; (B) Reports of federal, state and local agencies; (C) Reports of foreign agencies with whom DEA maintains liaison.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(4)(G), (H), (e)(5) and (8), (f), (g), (h) of the Privacy Act pursuant to 5 U.S.C. (j) and (k). Rules have been promulgated in accordance with the requirements of 5 U.S (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DEA-012

System name:

Registration Status/Investigation Records.

System location:

Drug Enforcement Administration, 1405 Eye Street NW, Washington, DC 20537. Also, field offices. See Appendix 1 for list of addresses.

Categories of individuals covered by the system:

Individuals who have a Controlled Substances Act registration number under their personal name who have had some action taken against their license or registration.

Categories of records in the system:

(A) DEA reports of investigation; (B) Information received from state regulatory agencies

Authority for maintenance of the system:

This system of records is maintained to enable the Drug Enforcement Administration to perform its regulatory functions under the Comprehensive Drug Abuse Prevention and Control Act of 1970.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information contained in this system of records is provided for law enforcement and regulatory purposes to the following categories of users on a routine basis: (A) Other federal law enforcement and regulatory agencies; (B) State and local law enforcement and regulatory agencies; (C) To respondents and their attorneys for purposes of discovery, formal and informal, in the course of an adjudicatory, rulemaking, or other hearing held pursuant to the Controlled Substances Act of 1970.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of Information to Members of Congress. Information contained in systems or records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

These records are maintained in standard case file folders.

Retrievability:

This system is indexed by name of registrant.

Safeguards:

This system of records is maintained in DEA Headquarters which is protected by 24-hour service and electronic surveillance. Access to the building is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. Access to the system is restricted to authorized employees of the Diversion Operations Section on a need-to-know basis.

Retention and disposal:

These records are retained as long as there is a need for the file. These are working files and may be destroyed when no longer required or merged into the Investigative Case File and Reporting System.

System manager(s) and address:

Deputy Assistant Administrator, Office of Diversion Control, Drug Enforcement Administration
1405 Eye Street, NW, Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to: Freedom of Information Section, Drug Enforcement Administration, 1405 I Street, NW, Washington, DC 20537.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

(A) DEA Investigators; (B) State and local regulatory agencies.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3), (d), (e)(4)(G) and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DEA-013

System name:

Security Files.

System location:

Drug Enforcement Administration, 1405 Eye Street, NW, Washington, DC 20537. Also, field offices. See Appendix 1 for list of addresses.

Categories of individuals covered by the system:

(A) DEA personnel; (B) Cooperating individuals and informants; (C) Drug traffickers and suspected drug traffickers; (D) Individuals who might discover DEA investigations or undercover operations by chance.

Categories of records in the system:

This system of records contains reports concerning the categories of individuals stated in

Authority for maintenance of the system:

This system of records is maintained to identify and correct security problems in the area

intelligence operations and installations pursuant to the Comprehensive Drug Abuse Prevention and Control Act of 1970 (Pub. L. 91-513) and Reorganization Plan No. 2 of

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

This system is utilized to generate reports on security problems in the area of intelligence operations and installations. In addition, information is provided to the following categories of users for law enforcement purposes on a routine basis: (A) Other federal law enforcement agencies; (B) State and local law enforcement agencies; (C) Foreign law enforcement agencies with whom DEA maintains liaison.

Release of information on the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

These records are maintained in standard case folders.

Retrievability:

The information in this system is retrieved by subject matter category or by coded identification number.

Safeguards:

This system of records is maintained at DEA Headquarters which is protected by twenty-four hour guard service and electronic surveillance. Access to the building is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. In addition, these records are stored in GSA approved security containers authorized for Secret material. Access to the system is restricted to authorized DEA personnel who have Top Secret Clearances on a limited need-to-know basis.

Retention and disposal:

Records in this system are retained as long as the individual remains active and then destroyed or retired to the Federal Records Center.

System manager(s) and address:

Deputy Assistant Administrator, Office of Intelligence, Drug Enforcement Administration
Eye Street, NW, Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to: Freedom of Information Section Drug Enforcement Administration, 1405 I Street, NW, Washington, DC 20537.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

(A) DEA Reports; (B) Reports of federal, state and local agencies.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(4)(G), (H), (e)(5) and (8), (f), (g), (h) of the Privacy Act pursuant to 5 U.S.C. (j) and (k). Rules have been promulgated in accordance with the requirements of 5 U.S (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DEA-014

System name:

System to Retrieve Information from Drug Evidence (STRIDE/Ballistics).

System location:

Drug Enforcement Administration, 1405 Eye Street, NW, Washington, DC 20537. Also, office. See Appendix 1 for list of addresses.

Categories of individuals covered by the system:

Defendants and suspected violators.

Categories of records in the system:

Ballistics report.

Authority for maintenance of the system:

This system is maintained to provide drug intelligence for law enforcement purposes pursuant to the Comprehensive Drug Abuse Prevention and Control Act of 1970 and Reorganization Plan No. 2 of 1973.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information from this system is provided to the following categories of users for law enforcement purposes on a routine basis: (A) Other federal law enforcement agencies; State and local law enforcement agencies; (C) Foreign law enforcement agencies with which DEA maintains liaison.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed for routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:***Storage:***

The information is stored on magnetic tape.

Retrievability:

The system is indexed by case number and exhibit number. The information can be retrieved by name of DEA case number and exhibit number. In addition, a number of telecommunications terminals have been added to the existing network.

Safeguards:

This system of records is maintained at DEA, headquarters which is protected by twenty-four hour guard service and electronic surveillance. Access to the building is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. Access to the system is restricted to authorized DEA employees with appropriate clearance on a need-to-know basis. Information that is retrievable by terminal requires user identification numbers which are issued to authorized employees of the Department of Justice.

Retention and disposal:

The information contained in this system is retained indefinitely.

System manager(s) and address:

Chief, Forensic Sciences Section, Drug Enforcement Administration; 1405 Eye Street, NW, Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to: Freedom of Information Section, Drug Enforcement Administration, 1405 I Street, NW, Washington, DC 20537.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

DEA Reports: Scientific Analysis.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(4)(G), (H), (e)(5) and (8), (f), (g), (h) of the Privacy Act pursuant to 5 U.S.C. (j). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 and (e) and been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DEA-015

System name:

Training Files.

System location:

Drug Enforcement Administration, 1405 I Street, NW, Washington, DC 20537 and DEA of Training, Federal Law Enforcement Training Center, Glynco, Georgia 31524.

Categories of individuals covered by the system:

Individuals who have attended training programs sponsored by the Drug Enforcement Administrative Office of Training.

Categories of records in the system:

(A) Students names; (B) Dates and locations of schools; (C) Class average and individual student grades; (D) Locations of student's employers; (E) Number of years experience in general law enforcement and drug law enforcement; (F) Classification of student's employment by state, local, county, or Federal; (G) Type of school attended; (H) Class rosters; (I)

Biographic data; (J) Evaluation reports; (K) Application and attendance records.

Authority for maintenance of the system:

This system is maintained to provide educational and training programs on drug abuse controlled substances law enforcement pursuant to the Comprehensive Drug Abuse Prevention and Control Act of 1970.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

This system is maintained to assist in performing the administrative functions of the Office of Training and is used to prepare class directories, class rosters, program evaluation reports, and statistical reports. In addition, information from this system is provided to Federal, state, and local law enforcement and regulatory agencies employing former students and biographic data may be provided to students and former students in the form of class rosters and publications.

Release of information to the news media: Information permitted to be released to the news media and the public may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information of Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional organization.

licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

The manual records in this system are maintained on index cards and in file folders and the automated portion is maintained on magnetic tapes.

Retrievability:

Data may be retrieved by the student's last name, school location code, or by beginning and ending dates.

Safeguards:

Those records maintained at DEA Headquarters are protected by twenty-four hour guard service and electronic surveillance. Access to the building is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. In addition, access to files is limited to Office of Training personnel on a need-to-know basis. Those records maintained at the Drug Enforcement Administration, Office of Training, FBI Academy Quantico, Virginia. Access to files is restricted to DEA personnel on a need-to-know basis.

Retention and disposal:

Records in this system are currently maintained indefinitely.

System manager(s) and address:

Deputy Assistant Administrator, Office of Training, Drug Enforcement Administration FBI Academy.

Notification procedure:

Inquiries should be addressed to: Freedom of Information Section, Drug Enforcement Administration, 1405 Eye Street NW, Washington, DC 20537.

Inquiries should contain name; date and place of birth; and dates of attendance at cour sponsored by the Office of Training.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

(A) Students: (B) Instructors.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/DEA-016***System name:***

Drug Enforcement Administration Accounting System (DEAAS II).

System location:

Drug Enforcement Administration, 1405 Eye Street NW, Washington, DC 20537. Also fi offices. See Appendix 1 for list of addresses.

Categories of individuals covered by the system:

All individuals who submit vouchers requesting payment for goods or services rendered payroll vouchers for DEA employees. These include vendors, contractors, experts, witnesses, court reporters, travelers, relocated employees, etc.

Categories of records in the system:

All vouchers paid except payroll vouchers for DEA employees. In addition all advance vouchers issued to DEA travelers.

Authority for maintenance of the system:

The system is established and maintained in accordance with the Budget and Accounting Procedures Act of 1950 as amended, 31 U.S.C. 66 and U.S.C. 200(a).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

After payment of the vouchers, the accounting data is used for the purpose of internal management reporting and external reporting to agencies such as OMB, U.S. Treasury, the GAO.

Release of information to the News Media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of Information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of Information to the National Archives and Records Administration (NARA) and

General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Manual voucher files are maintained alphabetically by payee's name. Travel advance information and other budget and accounting data are maintained by an online computer file. Information on travel advances is stored by employee identification number, other budget and accounting data is maintained by obligation number or other program identifier.

Retrievability:

Information from manual voucher files is retrieved by using the name of the payee. Travel advance information is retrieved by employee identification number; other budget and accounting data is retrieved by obligation number or other program identifier.

Safeguards:

Information contained in the system is unclassified. It is safeguarded in accordance with organizational rules and procedures. Access to manual voucher files is restricted to employees on a need to know basis. Information that is retrievable by terminals can be retrieved on authorized employees of the Department of Justice who have been issued user identification numbers.

Retention and disposal:

The payment documents are retained at this location for three fiscal years (current and prior years). The records are then shipped to a Federal Records Center for storage in accordance with the General Record Schedule published by the General Services Administration. In the computerized file for travel advances, only the last two transactions for any particular account are retained in the file. Old transactions are automatically purged and new transactions are entered.

System manager(s) and address:

Deputy Assistant Administrator, Office of Administration, Drug Enforcement Administration
1405 Eye Street NW, Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to Freedom of Information Section, Drug Enforcement Administration, 1405 Eye Street NW, Washington, DC 20537.

Record access procedures:

Same as "Notification Procedure" above.

Contesting record procedures:

Same as "Notification Procedure" above.

Record source categories:

Submitted by the payee involved.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/DEA-017

System name:

Grants of Confidentiality Files (GCF).

System location:

Drug Enforcement Administration, 1405 Eye Street, NW, Washington, DC 20537.

Categories of individuals covered by the system:

Applicants for grants of confidentiality.

Categories of records in the system:

(A) Requests for and actual Grants of Confidentiality; (B) Correspondence relating to at
(C) Documents relating to investigations of said applicants.

Authority for maintenance of the system:

Pursuant to 21 U.S.C. 872 of the Comprehensive Drug Abuse Prevention and Control A
1970.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information in these records are utilized for the purpose of investigating applicants prior granting of confidentiality. In the course of such investigations, information may be disseminated to state and local law enforcement and regulatory agencies to other federal enforcement and regulatory agencies.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specified information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed

a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

These records are maintained on standard case folders.

Retrievability:

The information in this system is retrieved by name of grantee.

Safeguards:

This system of records is maintained at DEA Headquarters which is protected by twenty-four hour guard service and electronic surveillance. Access to the building is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. In addition, the records are stored in bar lock filing cabinets and access to the system is restricted to members of the DEA employees on a "need to know basis."

Retention and disposal:

Records in this system are retained indefinitely.

System manager(s) and address:

Chief Counsel, Drug Enforcement Administration, 1405 Eye Street, NW, Washington, D.C. 20004

20537.

Notification procedure:

Inquiries should be addressed to: Freedom of Information Section, Drug Enforcement Administration, 1405 Eye Street, NW, Washington, DC 20537. Inquiries should include the inquirer's name, date, and place of birth.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

(A) DEA investigative reports; (B) Applicants; (C) Reports from other federal, state and local agencies.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (d)(1) and (e)(1) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DEA-018

System name:

DEA Applicant Investigations (DAI).

System location:

Drug Enforcement Administration; 1405 Eye Street, NW, Washington DC 20537.

Categories of individuals covered by the system:

Applicants for employment with DEA.

Categories of records in the system:

Information in records may include date and place of birth, citizenship, marital status, and social security status. These records contain investigative information regarding an individual's character, conduct, and behavior in the community where he or she lives or arrests and convictions for any violations against the law, information from inquiries directed to present and former supervisors, co-workers, associates, educators, etc, credit and National Agency checks, and other information developed from the above.

Authority for maintenance of the system:

5 U.S.C. 301 and Executive Order No. 10450.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records are used by DEA to implement an effective screening process for applicants from foreign, federal, state and local law enforcement and regulatory agencies, where appropriate for referral to avoid duplication of the investigative process and where the appropriate agency is charged with the responsibility of investigating or prosecuting potential violations of law.

Release of information to the news media. Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the

Member's behalf when the Member or staff requests the information on behalf of and at request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

These records are maintained in standard investigative folders.

Retrievability:

These records are retrieved by use of a card index maintained alphabetically by employee name.

Safeguards:

These records are maintained at DEA Headquarters which is protected by twenty-four hour guard service and electronic surveillance. Access to the building is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. Access to the system is restricted to employees of the office of Internal Security and upper level management officials. The records are stored in safe-type combination lock file cabinets.

Retention and disposal:

These records are maintained during period of employment and for 5 years after termination of employment and then destroyed.

System manager(s) and address:

Security Programs Manager, Drug Enforcement Administration, 1405 Eye Street, NW,

Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to: Freedom of Information Section, Drug Enforcement Administration, 1405 Eye Street, NW, Washington, DC 20537. Inquiries should include the inquirer's name, date, and place of birth.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

DEA investigations, federal, state and local law enforcement agencies.

Cooperating individuals, employees, educational institutions, references, neighbors, associates, credit bureaus, medical officials, probation officials.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsection (d)(1) and (e)(1) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5). Rules have been promulgated in accordance with the requirements at 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DEA-020

System name:

Essential Chemical Reporting System.

System location:

Drug Enforcement Administration (DEA), 1405 I Street, NW, Washington, DC 20537. Also Field Offices. See Appendix 1 for list of addresses.

Categories of individuals covered by the system:

- A. Individual who submit reports concerning the sale, loss, or theft of precursor or other chemical essential to the manufacture of controlled substances.
- B. Individuals who are reported as the purchaser, importer, or individual suffering the loss or theft of precursor or other chemical essential to the manufacture of controlled substances.
- C. Individuals who are reported as the person placing an order for precursor or other chemical essential to the manufacture of controlled substances.
- D. Individual who are reported as being involved in or having knowledge of the details relating to the loss or theft of precursor or other chemical essential to the manufacture of controlled substances.

Categories of records in the system:

The system contains: (1) Precursor diversion reports submitted to DEA pursuant to Pub. L. No. 95-633. (2) Information extracted from precursor reports and maintained on magnetic tape. Reports submitted voluntarily to DEA concerning chemicals essential to the manufacture of controlled substance.

Authority for maintenance of the system:

This system of records is maintained pursuant to the reporting requirements contained in Pub. L. 95-633.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information contained in this system is provided to the following categories of users for the

purposes stated:

(A) Other Federal law enforcement and regulatory agencies for law enforcement or regulatory purposes.

(B) State and local law enforcement and regulatory agencies for law enforcement and regulatory purposes.

(C) Release of information to the news media: Information permitted to be released to the media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(D) Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of the request of the individual who is the subject of the record.

(E) Release of information to the National Archives and Records Administration (NARA) and the General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to the NARA and GSA in management inspections under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Essential chemical report documents will be maintained in manual file folders. Information extracted will be maintained on magnetic tape.

Retrievability:

The information maintained on magnetic tape will be retrievable by the name of any individual mentioned in the report.

Safeguards:

The proposed system of records will be maintained in DEA Headquarters which is protected by twenty-four hour guard service and electronic surveillance. Access to the building is restricted to DEA employees and those persons transacting business within the building who are escorted by DEA employees. Manual files will be maintained in the DEA central files and access to these documents will be restricted to DEA employees on a need-to-know basis. Access to information maintained on magnetic tape will require a specific computer program to extract information. Access to information through ADP terminals will require a user identification code which will be issued to authorized DEA employees on a strict need-to-know basis.

Retention and disposal:

Until DEA gains experience to establish the useful life of the records in this system, the records will be maintained indefinitely.

System manager(s) and address:

Assistant Administrator for Operations, Drug Enforcement Administration, 1405 I Street NW, Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to Freedom of Information Section, Drug Enforcement Administration, 1405 I Street, NW, Washington DC 20537.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

Individuals required to submit precursor reports pursuant to Pub. L. 95–633, and individuals who voluntarily submit reports concerning the sale, distribution or importation of chemicals essential to the manufacture of controlled substances.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/DEA–021

System name:

DEA Aviation Unit Reporting System.

System location:

Drug Enforcement Administration (DEA), Investigative Support Section, Aviation Unit, DEA/Justice, PO Box 534, Addison, Texas 75001.

Categories of individuals covered by the system:

DEA pilots.

Categories of records in the system:

The system contains: (1) Records relating to the operation and maintenance of DEA aircraft. Records relating to pilot qualifications (CSC Form 671).

Purpose(s):

This system is maintained to monitor the utilization and maintenance of DEA aircraft and qualifications of DEA pilots in furtherance of DEA enforcement operations conducted pursuant to the Comprehensive Drug Abuse Prevention and Control Act of 1970 (Pub. L. 91-513)

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

- (1) Federal Aviation Administration for purposes of aircraft documentation and pilot certification.
- (2) Department of Defense for communication purposes.
- (3) United States Coast Guard for communication purposes.
- (4) Communications relay services under contract with DEA for communications purposes.
- (5) Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.
- (6) Release of information to Members of Congress. Information contained in the system records maintained by the Department of Justice, not otherwise requested to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of the Member at the request of the individual who is the subject of the record.
- (7) Release of information to the National Archives and Records Administration (NARA) and the General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes

responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system

Storage:

The automated portion of the records is maintained on an ADP disk storage device. Documentary records are maintained in manual file folders.

Retrievability:

Information relating to individuals in the system is retrieved by pilot name or identifying number assigned by DEA.

Safeguards:

Access to the system is restricted to DEA personnel on a need-to-know basis. The records are maintained in a secure room at the Addison Aviation Facility in accordance with DEA security procedures and are protected by an electronic alarm system.

Retention and disposal:

The automated records are maintained for five years and then purged from the data base. Manual records are maintained indefinitely.

System manager(s) and address:

Chief, Investigative Support Section, Drug Enforcement Administration, Washington, D.C. 20537.

Notification procedure:

Inquiries should be addressed to the Freedom of Information Section, Drug Enforcement Administration.

Administration, Washington, D.C. 20537.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

Information pertaining to individuals in the system is obtained from reports submitted by pilots.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/DEA-022

System Name:

EPIC Seizure System (ESS).

System Classification:

Sensitive But Unclassified.

System Location:

Department of Defense, Defense Information Systems Agency (DISA), Booz Allen Hami (contractor), 5201 Leesburg Pike, Suite 400, Falls Church, VA 22041, and Department of Justice, Drug Enforcement Administration, El Paso Intelligence Center, 11339 SSG Sim Street, El Paso, TX 79908-8098.

Categories of Individuals Covered by the System:

1. Categories consist of individuals identified or referenced in the course of investigation relating to:

(a) The illicit manufacture, distribution, sale or possession of, or trafficking in controlled substances;

(b) The illicit manufacture, distribution, sale or possession of, or trafficking in or alteration of identification documents, merchant mariner licenses and/or merchant mariner documents;

(c) Reports of lost, stolen or fraudulent use of identification documents;

(d) Businesses, vessels, and aircraft possibly associated with terrorism;

(e) Crewman desertions or stowaways;

(f) Movement of drugs, weapons, aliens or other contraband using vessels, commercial non-commercial aircraft, or vehicles;

(g) Tactical boarding of vessels suspected of smuggling drugs, weapons, aliens, or other contraband into the United States.

2. Categories also consist of individuals identified or referenced in requests for information:

(a) In support of U.S. Coast Guard and other law enforcement personnel conducting routine boardings;

(b) On crew lists of in-bound vessels that are 96 hours in advance of arrival to the United States;

(c) On personnel lists for individuals associated with work on or around Government or Government-contracted vessels;

(d) On personnel lists for individuals working in or around U.S. waterways, piers, and bridges.

(e) On pilots, passengers, owners, businesses and aircraft in support of Customs and Border Protection granting permission for aircraft to fly over the nearest Port of Entry;

(f) On Civil Air Patrol pilots supporting Drug Enforcement Administration or Immigration Customs Enforcement operations;

(g) On reported stolen aircraft.

Categories of Records in the System:

Records consist of:

(1) Personal identification and location data which may include name (including aliases and similar sounding names), occupation(s), race, sex, date and place of birth, height, weight, color, eye color, citizenship, nationality/ethnicity, alien status, addresses, and other miscellaneous identifying information, including, for example, telephone, passport, driver's license, vehicle registration, and Social Security numbers;

(2) Multi-source drug intelligence data;

(3) Counter-drug enforcement information, including identification, location, arrest, and prosecution of persons involved in the illicit trade or trafficking, and other activities and proceedings related to such enforcement activities;

(4) Information related to organizations involved in the illicit trade in controlled substances either in the United States or internationally;

(5) Reports of arrests;

(6) Information on stolen aircraft;

(7) Public and other information including personal identification and location data which include name, date and place of birth, social security numbers, addresses and other miscellaneous identifying information, including, for example, telephone numbers, driver's license, and vehicle registration obtained from commercial databases;

(8) Public and other information obtained from Federal warrants issued by United States Marshals Service;

(9) Vessel and aircraft data;

(10) Information relating to terrorist incidents;

(11) Other information involving the illicit possession, manufacture, sale, purchase, and transport of controlled substances; and

(12) Information involving the illicit manufacture, distribution, sale or possession of, trafficking in or alteration of identification documents, forged merchant mariner licenses and/or merchant mariner documents.

Authority for Maintenance of the System:

The Comprehensive Drug Abuse Prevention and Control Act of 1970 (83 Stat. 1236), Reorganization Plan No. 2 of 1973, the Omnibus Crime Control and Safe Streets Act, (F 90–351, as amended), and the Single Convention on Narcotic Drugs (18 U.S.C. 1407). Additional authority is derived from Treaties, Statutes, Executive Orders, Presidential Proclamations, and Attorney General Directives.

Purpose of the System:

Records in this system are used to provide investigative and public health and safety information for the Drug Enforcement Administration, and other law enforcement agencies in the discharge of their law enforcement duties and responsibilities.

Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses:

Pursuant to the Privacy Act, 5 U.S.C. 552a(b)(3), relevant records or any relevant facts contained therein may be disclosed:

(a) To Federal, state, local, tribal and foreign law enforcement agencies to facilitate the investigation and prosecution of illegal drug trafficking activities.

(b) To law enforcement individuals and organizations in the course of investigations where necessary to elicit information pertinent to counter-drug, counter-terrorism, weapons, and drug-money investigations.

(c) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or records.

(d) To a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, state, or local government entity or professional licensing authority in accordance with applicable regulations; or facilitating communications with a former employee that are necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter in that person's former area of responsibility.

(e) To the news media and the public, complying with 28 CFR 50.2 when applicable, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(f) To any criminal, civil, or regulatory law enforcement authority (whether Federal, state, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

(g) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

(h) To the National Archives and Records Administration (NARA) for purposes of managing inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(i) In an appropriate proceeding before a court or administrative or adjudicative body where records are determined by the Department of Justice to be arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(j) To agencies of the U.S. Intelligence Community.

Disclosure to Consumer Reporting Agencies:

None.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing Records in the System:

Storage:

Data is stored in electronic media via a configuration of personal computer, client/server mainframe systems architecture. Computerized records are maintained on hard disk, floppy diskettes, compact discs, magnetic tape, and/or optical disks. The records are stored on computer both at the contractor site and at the El Paso Intelligence Center, El Paso, Texas. Paper files are stored as follows: (1) In a secure file room with controlled access; (2) in locked file cabinets; and/or (3) in other appropriate GSA approved security containers.

Retrievability:

Records may be retrieved by reference to an individual's name or personal identifier.

Safeguards:

Both electronic and paper records are safeguarded in accordance with DOJ rules and policies governing automated systems security and access. These safeguards include the maintenance of technical equipment in restricted areas, and the required use of individual passwords and user identification codes to access the system. The system is protected by both physical security methods and dissemination and access controls. Protection of the automated information system is provided by physical, procedural and electronic means.

Retention and Disposal:

Records in this system will be retained and disposed of in accordance with records schedules approved by the National Archives and Records Administration (NARA) for the constituent systems of records, Justice/DEA-002 and Justice/DEA-INS-111. A separate schedule for retention and disposal of records for Justice/DEA-022 will be submitted to NARA for approval.

System Manager and Address:

Director, El Paso Intelligence Center, 11339 SSG Sims Street, El Paso, Texas 79912-80

Notification Procedures:

Inquiries should be addressed to Freedom of Information and Records Section, Drug Enforcement Administration, Washington, DC 20537.

Record Access Procedures:

A request for access to a record from this system shall be made in accordance with 28 (part 16 to the Freedom of Information Act (FOIA)/Privacy Act (PA) Section, Headquarter Enforcement Administration, Washington, DC 20537 or to the System Manager, with the envelope and letter clearly marked 'Privacy Access Request.' The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury and dated. Some information may be exempt from access to certain provisions as described in the section entitled 'Exemptions Claimed for the System.' An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

Contesting Record Procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Record Access Procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment. Some information may be exempt from contesting record procedures as described in the section entitled 'Exemptions Claimed for the System.' An individual who is the subject of a record in this system may seek amendment of those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

Record Source Categories:

(1) DEA intelligence and investigative records; (2) reports, investigative and intelligence

from other participating and associated Federal, state, local, territorial, tribal, and foreign member agencies; (3) records and reports of foreign law enforcement and regulatory agencies; and (4) records from commercial databases.

Exemptions Claimed for the System:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d)(1), (2) and (4); (e)(1), (2) and (3), (e)(5) and (e)(8); and (g), of the Privacy Act pursuant to 5 U.S.C. 552a(j) and (k). The exemptions will be applied only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k). A determination as to whether a record shall be made at the time a request for access or amendment is received. Proposed rule has been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and published in today's *Federal Register*.

[\[TOP\]](#)

JUSTICE/DEA-023

System name:

Clerical, Technical and Professional (CTAP) Program Files.

System location:

Drug Enforcement Administration, 1405 I Street, NW, Washington, DC 20537 and field offices (see Appendix 1 for addresses).

Categories of individuals covered by the system:

Clerical technical and professional employees (GS/1-12) of DEA who volunteer to participate in the CTAP program.

Categories of records in the system:

Biographic, educational and career development records of CTAP employees, interview evaluation forms concerning CTAP employees and individual career development plans

Authority for maintenance of the system:

OMB Circular No. A-48 (September 23, 1971). Federal Personnel Manual, Chapter 410

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information is disclosed to DEA counselors and supervisors to develop and plan individual career development programs for DEA employees.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2, may be made available from systems of records maintained by the Department of Justice unless it is determined that release of specific information in the context of a particular case would constitute an unwarranted invasion of personnel privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise requested to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests that information on behalf of and a request of the individual who is the subject of the record.

Release of information to the National Archives and Record Administration (NARA) and General Service Administration (GSA): A record from a system of records may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C 2904 and 2906.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:***Storage:***

The records in the system are maintained in manual file folders and on ADP equipment

Retrievability:

Records will be retrieved by employee name.

Safeguards:

The records in the system will be maintained in facilities which meet DEA security requirements. Access to the system will be restricted to DEA employees on a need-to-know basis.

Retention and disposal:

Indefinite.

System manager(s) and address:

Assistant Administrator, Office of Administration, Drug Enforcement Administration, 1405 I Street, NW, Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to Freedom of Information Section, Drug Enforcement Administration, 1405 I Street, NW, Washington, DC 20537.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

DEA employees, CTAP Counselors, DEA personnel files.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/DEA-027

System name:

DEA Employee Profile System (DEPS).

System location:

Drug Enforcement Administration, 1405 I Street, NW, Washington, DC 20537.

Categories of individuals covered by the system:

DEA employees.

Categories of records in the system:

The following eight categories of information will be maintained in the system:

1. Personal identification
2. Work experience
3. Language & geographical areas
4. Formal education
5. Special skills
6. Record of training
7. Consideration for vacancies
8. Awards

Authority for maintenance of the system:

This system is maintained to effectively place and assign employees to positions to further mandates of the Comprehensive Drug Abuse Prevention and Control Act of 1970.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The records will be used principally by the Personnel Management Division. Selected data will be forwarded by this personnel section to the Career Development Board and operation throughout DEA for the purpose of:

1. Identifying employees with particular skills or qualifications for assignment to special projects.
2. Identification of candidates for overseas assignments who have specific language skills.
3. Insuring that the Career Development Board will be reviewing the entirety of an applicant's background.
4. Calculating DEA's human resources on hand and to project more accurately future recruitment needs and capabilities.

Information from this system will not be disseminated outside of DEA.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:***Storage:***

These records will be maintained on magnetic tape and a disk storage device.

Retrievability:

The information in this system can be retrieved by the individual's name, special skills information, special knowledge information or by some combination of the above inform

Safeguards:

The records of the system will be maintained at DEA Headquarters which is protected by twenty-four hour guard service and electronic surveillance. Access to the building is restricted to DEA employees and those transacting business within the building who are escorted by DEA employees. In addition, the area where the tapes and disks are stored is a secure area and access is restricted to those employees who have business in the area and those non-employees who are transacting business within the area and escorted by a DEA employee. Inquiries to the system are only made by the written request of the Chief, Personnel Management Division.

Retention and disposal:

Records in this system are retained as long as the individual is employed by DEA.

System manager(s) and address:

Deputy Assistant Administrator, Office of Administration, Drug Enforcement Administration
1405 I Street NW, Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to Freedom of Information Section, Drug Enforcement Administration, 1405 I Street NW, Washington, DC 20537. Inquiries should include inquiry name, date of birth, and social security number.

Record access procedures:

Same as notification procedure.

Contesting record procedures:

Same as Notification Procedures

Record source categories:

1. DEA employee
2. Servicing personnel Office
3. The Justice Uniform Personnel System (Juniper).

Systems exempted from certain provisions of the act: None.

[\[TOP\]](#)

JUSTICE/DEA-028

System name:

Regional Automated Intelligence Data System (RAIDS).

System location:

Drug Enforcement Administration, 8400 NW 53rd Street, Miami, Florida 33166.

Categories of individuals covered by the system:

Individuals suspected of illicit narcotic trafficking.

Categories of records in the system:

Information extracted from DEA investigative reports.

Authority for maintenance of the system:

The Comprehensive Drug Abuse Prevention and Control Act of 1970 (Pub. L. 91-513).

Routine uses of records maintained in the system, including categories of users and

purposes of such uses:

Information contained in this system is provided to the following categories of users as a part of routine use for law enforcement and regulatory purposes: (a) Other federal law enforcement and regulatory agencies; (b) State and local law enforcement and regulatory agencies; (c) Foreign law enforcement agencies with whom DEA maintains liaison; (d) The Department of Defense and military departments; (e) The Department of State; (f) United States intelligence agencies concerned with drug enforcement; (g) The United Nations; (h) The International Police Organization (Interpol); and (i) To individuals and organizations in the course of investigations to elicit information.

In addition, disclosures are routinely made to the following categories for the purposes of: (a) To federal agencies for national security clearance purposes and to federal and state regulatory agencies responsible for the licensing or certification of individuals in the field of pharmacy and medicine; (b) To the Office of Management and Budget, upon request, in order to justify the allocation of resources; (c) To state and local prosecutors for assistance in preparing cases concerning criminal and regulatory matters; and (d) To respondents and attorneys for purposes of discovery, formal and informal, in the course of an adjudicator's rulemaking, or other hearing held pursuant to the Controlled Substances Act of 1970.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspection conducted under the authority of U.S.C. 2904 and 2906.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Records in the system are maintained on magnetic discs.

Retrievability:

Information is retrieved by name of the subject and by various topical queries.

Safeguards:

The system is protected by both physical security and dissemination and access control system is maintained in a secure DEA facility and protected by electronic means. Access computer is restricted by the assignment of unique input and query access codes to DEA employees on a strict need-to-know basis.

Retention and disposal:

Records in the system are currently maintained indefinitely.

System manager(s) and address:

Regional Director, DEA South Eastern Regional Office, 8400 NW, 53rd Street, Miami, FL 33166.

Notification procedure:

Inquiries should be addressed to: Freedom of Information Unit, Drug Enforcement Administration, 1405 I Street, NW, Washington, DC 20537.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

Records in the system consist entirely of information extracted from DEA investigative re

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) (2), and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), (g) and (h) of the Privacy Act pursuant to U.S.C. 552a (j) and (k). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e).

[\[TOP\]](#)

JUSTICE/DEA-030

System name:

Agent Recruit Assessment Program.

System location:

Drug Enforcement Administration (DEA), 1405 I Street, NW, Washington, DC 20537.

Categories of individuals covered by the system:

- A. Prospective recruits for basic agent classes
- B. Basic agent trainees
- C. Special Agents

Categories of records in the system:

The system contains information concerning: (1) Scores on measurement instruments; (2) personality score derivatives; and (3) job-related factors.

Authority for maintenance of the system:

This system is maintained under DEA's authority to recruit and train Special Agents to enforce the Comprehensive Drug Abuse Prevention and Control Act of 1970 (Pub. L. 91-513).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The records maintained in this system are utilized only for internal purposes and no dissemination outside the Department of Justice is contemplated.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:***Storage:***

The automated portion of the records is maintained on an ADP storage device. Document records are maintained in manual file folders.

Retrievability:

Information relating to an individual is retrieved by name or a unique identifying number assigned by DEA.

Safeguards:

Access to the system is restricted to DEA personnel on a strict need-to-know basis. The records are maintained in a secure area at DEA headquarters, which is protected by guard and electronic means.

Retention and disposal:

The automated portion of the system is maintained for 15 years and then purged from the database. Manual records are maintained indefinitely.

System manager(s) and address:

Assistant Administrator for Enforcement, Drug Enforcement Administration, 1405 I Street
Washington, DC 20537.

Notification procedure:

Inquiries should be addressed to: Freedom of Information Division, Drug Enforcement
Administration, 1405 I Street, NW, Washington, DC 20537.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

Information pertaining to individuals in the system is obtained from test protocols and al
records or provided by the individuals.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (d), (e)(4)(G) and (H)
(f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(6). See 28 CFR 16.98 for exemption
regulations.

[\[TOP\]](#)

JUSTICE/DEA-999

DEA Appendix 1—List of record location addresses. Copies of all or part of any system
records published by the Drug Enforcement Administration pursuant to 5 U.S.C. 552a n
maintained at the DEA field offices listed below. However, procedures for processing inq
concerning DEA systems of records have been centralized in DEA Headquarters. Inquir
concerning all DEA systems of records should be addressed to:

Freedom of Information Section:

Drug Enforcement Administration, 1405 Eye Street, NW, Washington, DC 20537.

Drug Enforcement Administration Field Offices:

Atlanta Division

Atlanta Division Office, 75 Spring Street, SW, Room 740, Atlanta, Georgia 30303

Charleston Resident Office, 334 Meeting Street, Room 325, Charleston, South Carolina

Columbia Resident Office, 1101 Laurel, PO Box 702, Room 204, Columbia, South Carolina 29202

Columbus Resident Office, PO Box 1565, Columbus, Georgia 31902

Greensboro Resident Office, 2300 W. Meadowview Road, Suite 224, Greensboro, North Carolina 27407

Knoxville Resident Office, 1111 Northshore Drive, Room 610, Knoxville, Tennessee 379

Memphis Resident Office, 167 N. Main Street, 401 Federal Building, Memphis, Tennessee 38103

Nashville Resident Office, 801 Broadway, A929, Estes Kefauver Building, FB-USCH, Nashville, Tennessee 37203

Savannah Resident Office, 124 Barnard Street, Room B-220, Savannah, Georgia 3140

Wilmington Resident Office, 272 Front Street, Suite 423, Wilmington, North Carolina 28

Boston Division

Boston Division Office, G-64 JFK Federal Building, Boston, Massachusetts 02203

Bridgeport Resident Office, 915 Lafayette Boulevard, FB-USCH, Room 200, Bridgeport,

Connecticut 06604

Burlington Resident Office, PO Box 327, Essex Junction, Vermont 05452

Concord Resident Office, 55 Pleasant Street, Federal Building, PO Box 1314, Concord, Hampshire 03301

Hartford Resident Office, 450 Main Street, Room 628, Hartford, Connecticut 06103

Portland Resident Office, 1355 Congress Street, Suite D, Portland, Maine 04102

Providence Resident Office, 232 John O. Pastore Federal Building, Exchange Terrace, Providence, Rhode Island 02903

Springfield Resident Office, 1550 Main Street, Room 408, Springfield, Massachusetts 01103

Chicago Division

Chicago Division Office, 219 Dearborn Street, Chicago, Illinois 60604

Fargo Resident Office, PO Box 1127, Fargo, North Dakota 58107

Hammond Resident Office, 507 State Street, Room 632, Hammond, Indiana 46320

Indianapolis Resident Office, 575 N. Pennsylvania, Room 290, Indianapolis, Indiana 46204

Milwaukee Resident Office, 517 E. Wisconsin, 228A FB-USCH, Milwaukee, Wisconsin 53201

Minneapolis Resident Office, 110 S. 4th Street, 402 Federal Building, Minneapolis, Minnesota 55401

Springfield Resident Office, 524 S. Second Street, Suite 650, Springfield, Illinois 62701

Dallas Division

Dallas Division Office, 1880 Regal Row, Dallas, Texas 75235

Fort Worth Resident Office, 501 W. 10th Street, U.S. Courthouse, Room 506, Fort Worth Texas 76102

Oklahoma City Resident Office, 200 NW Fifth Street, Federal Building, Suite 960, Oklahoma City, Oklahoma 73102-3202

Tulsa Resident Office, 333 W. Fourth Street, Room 3335, Tulsa, Oklahoma 74103

El Paso Resident Office, 4110 Rio Bravo, Suite 100, El Paso, Texas 79902

Alpine Resident Office, PO Box 1282, Alpine, Texas 79830

Lubbock Resident Office, 2345 50th Street, Suite 120, Lubbock, Texas 79412

Midland, Texas, Post of Duty, 200 E. Wall, Federal Building, Room 105, Midland, Texas

Tyler, Texas, Post of Duty, 3301 Golden Road No. 5, Tyler, Texas 75713

Denver Division

Denver Division Office, 316 US Customs House, PO Box 1860, Denver, Colorado 80201

Cheyenne Resident Office, 2120 Capitol Avenue, 8020 Federal Center, Cheyenne, WY 82001

Salt Lake City Resident Office, 125 State Street, 8416 Federal Building, Salt Lake City, 84138

Albuquerque District Office, 5301 Central Avenue NE., 1st National Bank Building East, 900, Albuquerque, New Mexico 87108

Glenwood Springs Resident Office, 401 23rd Street, Suite 104, Glenwood Springs, Colorado 81601

Las Cruces Resident Office, PO Box 399, Las Cruces, New Mexico 88004

Detroit Division

Detroit Division Office, 231 W. Lafayette, 357 Federal Building, Detroit, Michigan 48226

Cincinnati Resident Office, 505 Main Street, 7405 Federal Office Building, Cincinnati, O 45202

Cleveland Resident Office, 601 Rockwell Avenue, Room 300, Cleveland, Ohio 44114

Grand Rapids Resident Office, 110 Michigan Avenue, NW, 310 FB-USCH, Grand Rapids, Michigan 49503

Louisville Resident Office, 600 Federal Place, 1006 Federal Building, Louisville, Kentucky 40202

Saginaw Resident Office, 100 S. Warren Street, Room 1061, Federal Building, Saginaw, Michigan 48606

Houston Division

Houston Division Office, 333 West Loop North, Houston, Texas 77024

Corpus Christi Resident Office, 400 Mann Street, PO Box 2443, Suite 403, Corpus Christi, Texas 78403

Galveston Resident Office, 6000 Broadway, Suite 104, Galveston, Texas 77550

Beaumont, Texas, Post of Duty, 700 North Street, Suite 102, Beaumont, Texas 77701-1

McAllen District Office, 3017 S. 10th Street, McAllen, Texas 78503

Brownsville, Resident Office, 1100 FM 802, Suite, 200, Brownsville, Texas 78521

Laredo Resident Office, PO Box Drawer 2307, Laredo, Texas 78044

San Antonio Resident Office, 1802 NE Loop 410, 1800 Central Building, 4th Floor, San Antonio, Texas 78205

Antonio, Texas 78217

Austin Resident Office, 55 N. Interregional Highway, PO Box 8, Austin, Texas 78767

Eagle Pass Resident Office, 342 Rio Grande, Room 102, Eagle Pass, Texas 78852

Los Angeles Division

Los Angeles Division Office, 305 S. Figueroa Street, Los Angeles, California 90071

Guam Resident Office, 238 O'Hara Street, Suite 502C, Agana, Guam 96910

Honolulu Resident Office, 300 Ala Moana Boulevard, Room 3129, PO Box 50163, Honolulu, Hawaii 96850

Las Vegas Resident Office, 300 Las Vegas Boulevard South, FB-USCH, Room 204, PC 16023, Las Vegas, Nevada 89101-0023

Reno Resident Office, 4600 Kietzke Lane, 209 Building I, Reno, Nevada 89502

Riverside Resident Office, 3610 Central Avenue, Room 511, PO Box 2946, Riverside, California 92516

Santa Ana Resident Office, 34 Civic Center Plaza, PO Box 12609, Santa Ana, California

Santa Barbara Resident Office, 6445 Calle Real, Suite C, Goleta, California 93117

Miami Division

Miami Division Office, 8400 NW 53rd Street, Miami, Florida 33166

Ft. Lauderdale Resident Office, 299 E. Broward Boulevard, FB-USCH, Suite 404, Ft. Lauderdale, Florida 33301

Ft. Myers Resident Office, 2345 Union Street, Suite D, Ft. Myers, Florida 33902

Gainesville Resident Office, 1717 NE 9th Street, Suite 134, PO Box 2918, Gainesville, Florida

32601

Jacksonville Resident Office, 4077 Woodcock Drive, Suite 210, Jacksonville, Florida 322

Marathon Resident Office, 11400 Overseas Highway, PO Box 1269, Room 215, Marathon, Florida 33050

Orlando Resident Office, 498 Palm Springs Plaza Drive, Suite 801, Altamonte Springs, Florida 32701

Panama City Resident Office, 410 Jenks Avenue, PO Box 1486, Panama City, Florida 32301

Tampa Resident Office, 700 Twiggs Street, Suite 400, Tampa, Florida 33602

Tampa Task Force Airport Detail, 700 Twiggs Street, Suite 400, Tampa, Florida 33602

West Palm Beach Resident Office, 701 Clematis Street, Room 223, West Palm Beach, Florida 33401

San Juan District Office, 416 Ponce de Leon Avenue, Chase Building, Suite 514, Hato Rey, Puerto Rico 00918

Newark Division

Newark Division Office, 970 Broad Street, Federal Office Building, Room 806, Newark, New Jersey 07102

Atlantic City Resident Office, PO Box AB, Northfield, New Jersey 08225

Camden, New Jersey Resident Office, c/o DEA, PO Box 428, Bellmawr, New Jersey 08031

New Orleans Division

1661 Canal Street, Suite 2200, New Orleans, Louisiana 70112

Baton Rouge Resident Office, 4560 North Boulevard, Suite 118, Baton Rouge, Louisiana 70802

Birmingham Resident Office, 236 Goodwin Crest, Suite 520, Birmingham, Alabama 35201

Gulfport Mississippi, Post of Duty, PO Box 1387, Gulfport, Mississippi 39502

Jackson Resident Office, 100 W. Capitol Street, 1501 Federal Building, Jackson, Mississippi 39269

Little Rock Resident Office, One Union National Plaza, Suite 850, Little Rock, Arkansas 72201

Mobile Resident Office, 2 Office Park, Suite 216, Mobile, Alabama 36609

Shreveport Resident Office, 8A20A Federal Building, Shreveport, Louisiana 71101

New York Division

New York Division Office, 555 W. 57th Street, Suite 1900, New York, New York 10019

Albany Resident Office, Clinton Avenue & North Pearl Street, 746 Leo W. O'Brien Federal Building, Albany, New York 12207

Buffalo Resident Office, 28 Church Street, Suite 300, Buffalo, New York 14202

Rochester Resident Office, PO Box 14210, Rochester, New York 14614

Long Island Resident Office, One Huntington Quadrangle, Suite 1C-02, Melville, New York 11747

New York DEA Drug Task Force, 555 W. 57th Street, Suite 1700, New York, New York 10019-2978

JFK Airport Station, PO Box 361, Jamaica, New York 11430

Philadelphia Division

Philadelphia Division Office, 600 Arch Street, Room 10224, William J. Green Federal Building, Philadelphia, Pennsylvania 19106

Harrisburg Resident Office, PO Box 557, Harrisburg, Pennsylvania 17108–0557

Pittsburgh Resident Office, 1000 Liberty Avenue, Federal Building, Room 2306, Pittsburgh, Pennsylvania 15222

Wilmington Resident Office, 844 King Street, J. Caleb Boggs Federal Building, Rms. 5305–5307, Wilmington, Delaware 19801

Phoenix Division

Phoenix Division Office, One N. First Street, Suite 201, Phoenix, Arizona 85004

Yuma Resident Office, 3150 Winsor Avenue, Suite 202, Yuma, Arizona 85364

Tucson Resident Office, 2110 E. Airport Drive, Tucson, Arizona 85706

Nogales Resident Office, 3970 Fairway Drive, Nogales, Arizona 85621

San Diego Division

San Diego Division Office, 402 W. 35th Street, National City, California 92050

Calexico Resident Office, 38 W. 4th Street, PO Box J, Calexico, California 92231

Tecate Resident Office, Highway 188, PO Box 280, Tecate, California 92080

San Francisco Division

San Francisco Division Office, 450 Golden Gate Avenue, PO Box 36035, Room 12215, San Francisco, California 94102

Fresno Resident Office, 2202 Monterrey Street Room, 104F, Fresno, California 93721

Sacramento Resident Office, 2941 Fulton Avenue, PO Box 214556, Sacramento, California 95821

San Jose Resident Office, 280 S. First Street, Room 2133, San Jose, California 95113

Seattle Division

Seattle Division Office, 220 W. Mercer, Suite 301, Seattle, Washington 98119

Anchorage Resident Office, 701 C Street, Anchorage, Alaska 99513

Blaine Resident Office, 170 C Street, PO Box 1680, Blaine, Washington 98230

Boise Resident Office, 2404 Bank Drive, American Reserve Building, Suite 212, Boise, ID 83705

Eugene Resident Office, 211 E. 7th Avenue, 230 Federal Building, Eugene, Oregon, 97

Great Falls Resident Office, 1111 4th Street South, PO Box 2887, Great Falls, Montana

Portland Resident Office, 1220 SW 3rd Avenue, Room 1566, Portland, Oregon 97204

Spokane Resident Office, 920 W. Riverside, PO Box 1504, USCH, Spokane, Washington 99201

St. Louis Division

St. Louis Division Office, 120 S. Central Avenue, Suite 200, St. Louis, Missouri 63105

Cape Girardeau, Missouri, Post of Duty, 339 Broadway, Room 159, Cape Girardeau, Missouri 63701

Des Moines Resident Office, 210 Walnut Street, PO Box 1784, USCH, Federal Building 667, Des Moines, Iowa 50309

Kansas City Resident Office, 812 N. 7th Street, Room 206, Kansas City, Kansas 66101

Omaha Resident Office, 215 N. 17th Street, Federal Building, PO Box 661, Downtown Omaha, Nebraska 68101

Sioux Falls Resident Office, PO Box 1109, Sioux Falls, South Dakota 57101

Wichita Resident Office, 1919 Amidon, Suite 218, Wichita, Kansas 67230

Washington, DC Division

Washington, DC Division Office, 400 Sixth Street SW., Room 2558, Washington, DC 20

Charleston Resident Office, 22 Capital Street, PO Box 1146, Charleston, West Virginia :

Clarksburg, West Virginia, Post of Duty, 168 W. Main Street, PO Box 262, Room 502,
Clarksburg, West Virginia 26301

Charleston Resident Office, 22 Capital Street, PO Box 1146, Charleston, West Virginia :

Norfolk Resident Office, 200 Granby Mall, Federal Building, Suite 320, Norfolk, Virginia

Richmond Resident Office, 400 N. 8th Street, PO Box 10150, Richmond, Virginia 23240

Baltimore District Office, 31 Hopkins Plaza, 955 Federal Building, Baltimore, Maryland 2

El Paso Intelligence Division

El Paso Intelligence Division, 2211 E. Missouri, Suite 200, El Paso, Texas 79903

Laboratories

Special Testing & Research Laboratory, 7704 Old Springhouse Road, McLean, Virginia
22102-3494

Mid-Atlantic Laboratory, 460 New York Avenue NW, Washington, DC 20537

Northeast Laboratory, 555 W. 57th Street, New York, New York 10019

Southeast Laboratory, 5205 NW 84th Avenue, Miami, Florida 33166

North Central Laboratory, 610 S. Canal Street, Room 500, Chicago, Illinois 60607

South Central Laboratory, 1880 Regal Row, Dallas, Texas 75235

Southwest Laboratory, PO Box 1536, National City, California 92050

Western Laboratory, 450 Golden Gate Avenue, Box 36075, San Francisco, California 94

Other DEA Offices

Aviation Unit

Addison Aviation Facility, DEA/Justice, PO Box 534, Addison, Texas 75001

Foreign Offices

Ankara, Turkey Country Office, DEA/Justice, American Embassy, APO New York, New York 09254

Istanbul Resident Office, DEA/Justice, American Consulate General, APO New York, New York 09380

Athens Greece Country Office, DEA/Justice, American Embassy, APO New York, New York 09253

Bangkok, Thailand Country Office, DEA/Justice, American Embassy, APO San Francisco, California 96346

Chiang Mai Resident Office, DEA/Justice, American Embassy, Box C, APO San Francisco, California 96346

Songkhla Resident Office, DEA/Justice, American Embassy, Box S, APO San Francisco, California 96346

Bern, Switzerland Country Office, DEA/Justice, American Embassy, Department of State, Bern, Switzerland 20520

Bogota, Colombia Country Office, DEA/Justice, American Embassy, APO Miami, Florida

Barranquilla Resident Office, DEA/Justice, American Embassy, APO Miami, Florida 340

Cali Resident Office, DEA/Justice, American Embassy, APO Miami, Florida 34038

Medellin Resident Office, DEA/Justice, American Embassy, APO Miami, Florida 34038

Bonn, W. Germany Country Office, DEA/Justice, American Embassy, Box 290, APO New York 09080

Frankfurt Resident Office, DEA/Justice, American Consulate General, APO New York, New York 09213

Brasilia, Brazil Country Office, DEA/Justice, American Embassy, APO Miami, Florida 340

Sao Paulo Resident Office, c/o Brasilia Country Office, APO Miami, Florida 34030

Brussels, Belgium Country Office, DEA/Justice, American Embassy, APO New York, New York 09667

Buenos Aires, Argentina Country Office, DEA/Justice, American Embassy, APO Miami, Florida 34034

Cairo, Egypt Country Office, DEA/Justice, American Embassy, Box 10, FPO New York, New York 09527

Caracas, Venezuela Country Office, DEA/Justice, American Embassy, APO Miami, Florida 34037

Copenhagen, Denmark Country Office, DEA/Justice, American Embassy, APO New York, New York 09170

Caracao, Netherlands Antilles Country Office, DEA/Justice, c/o U.S. Consulate General
Department of State Pouch Mail 20520

Guatemala City, Guatemala Country Office, DEA/Justice, American Embassy, APO Miami, Florida 34024

Hong Kong Country Office, DEA/Justice, American Consulate General, Box 30, FPO San Francisco, California 96659

Islamabad, Pakistan Country Office, DEA/Justice, Department of State, Pouch Mail 20520

Karachi Resident Office, DEA/Justice, Department of State, Pouch Mail 20520

Lahore Resident Office, DEA/Justice, Department of State, Pouch Mail 20520

Peshawar Resident Office, DEA/Justice, Department of State, Pouch Mail 20520

Jakarta, Indonesia Country Office, DEA/Justice, Department of State, Pouch Mail 20520

Kingston, Jamaica Country Office, DEA/Justice, Department of State, Pouch Mail 20520

Kuala Lumpur, Malaysia Country Office, DEA/Justice, Department of State, Pouch Mail 20520

La Paz, Bolivia Country Office, DEA/Justice, American Embassy, APO Miami, Florida 34031

Santa Cruz Resident Office, c/o La Paz, Bolivia Country Office, APO Miami, Florida 34031

Lagos, Nigeria Country Office, DEA/Justice, Department of State, Pouch Mail 20520

Cochabamba Resident Office, c/o La Paz, Bolivia Country Office, APO Miami, Florida 34031

Lima, Peru Country Office, DEA/Justice, American Embassy, APO Miami, Florida 34031

London, England Country Office, DEA/Justice, American Embassy, Box 40, FPO New York, New York 09510

Madrid, Spain Country Office, DEA/Justice, American Embassy, APO New York, New York 09285

Manila, Philippines Country Office, DEA/Justice, American Embassy, APO San Francisco
California 96528

Mexico City, Mexico Country Office, DEA/Justice, PO Box 3087, Laredo, Texas 78041

Guadalajara Resident Office, DEA/Justice, PO Box 3088, Laredo, Texas 78041

Hermosillo Resident Office, PO Box 1090, Nogales, Arizona 85621

Mazatlan Resident Office, DEA/Justice, Department of State, Pouch Mail 20520

Merida Resident Office, DEA/Justice, American Consulate, PO Box 3087, Laredo, Texas

Monterrey Resident Office, DEA/Justice, American Consulate, PO Box 3098, Laredo, Texas
78040

Nassau, Bahamas Country Office, DEA/Justice, PO Box N8197, Department of State, Pouch
Mail 20520

New Delhi, India Country Office, DEA/Justice, American Consulate, Department of State
Pouch Mail 20520

Nicosia, Cypress Country Office, DEA/Justice, American Embassy, FPO New York, New York
09530

Ottawa Country Office, 100 Wellington Street, DEA/Justice, American Embassy, Ottawa
Ontario, Canada K1P-5T1

Montreal Resident Office, DEA/Justice, PO Box 65, Postal Station, Desjardins, Montreal
American Consulate General, Montreal, Quebec, Canada H3B 1G1

Panama City, Panama Country Office, DEA/Justice, American Embassy, Box E, APO Miami
Florida 34002

Paris, France Country Office, DEA/Justice, American Embassy, APO New York, New York

09777

Marseilles Resident Office, DEA/Justice, American Embassy, APO New York, New York

Quito, Ecuador Country Office, DEA/Justice, American Embassy, APO Miami, Florida 34

Guayaquil Resident Office, DEA/Justice, U.S. Consulate, APO Miami, Florida 34039

Rome, Italy Country Office, DEA/Justice, American Embassy, APO New York, New York
09794-0007

Milan Resident Office, DEA/Justice, American Embassy, Box M, APO New York, New York
09794

San Jose, Costa Rica Country Office, DEA/Justice, American Embassy, APO Miami, Florida
34020

Santiago, Chile Country Office, DEA/Justice, American Embassy, APO Miami, Florida 34

Santo Domingo, Dominican Republic Country Office, DEA/Justice, American Embassy,
Miami, Florida 34041

Seoul, Korea Country Office, DEA/Justice, American Embassy, APO San Francisco, California
96301

Singapore Country Office, DEA/Justice, American Embassy, FPO San Francisco, California
96699-0001

The Hague, Netherlands Country Office, DEA/Justice, American Embassy, APO New York, New York
09159

Tokyo, Japan Country Office, DEA/Justice, American Embassy, APO San Francisco, California
96503

Vienna, Austria Country Office, DEA/Justice, American Embassy, APO New York, New York
09108

[\[TOP\]](#)

Executive Office for Immigration Review

JUSTICE/EOIR-001

System name:

Records and Management Information System (JUSTICE/EOIR-001).

Security Classification:

Not classified.

System location:

Executive Office for Immigration Review, Department of Justice, 5107 Leesburg Pike 2600, Falls Church, Virginia 22041. The system is also located in EOIR field offices. EOIR Web site, <http://www.usdoj.gov/eoir/>, maintains a current address listing of all field offices.

Category of Individuals covered by the system:

This system contains case-related information pertaining to aliens and alleged aliens brought into the immigration hearing process, including certain aliens previously or subsequently admitted for lawful permanent residence. The system also includes information pertaining to attorneys and representatives practicing before Immigration Judges and the Board of Immigration Appeals.

Categories of records in the system:

This system includes the name, file number, address and nationality of aliens and alleged aliens, decision memoranda, investigatory reports and materials compiled for the purpose of enforcing immigration laws, exhibits, transcripts, and other case-related papers concerning aliens, alleged aliens or lawful permanent residents brought into the administrative adjudication process. The system also includes electronic records of names, birth dates, last four (4) digits of social security number, bar membership, addresses, including electronic addresses, of attorneys and representatives practicing before Immigration Judges and the Board of Immigration Appeals.

before Immigration Judges, and the Board of Immigration Appeals.

Authority for Maintenance of the System:

This system is established and maintained under the authority granted the Attorney pursuant to 44 U.S.C. 3101 and 3103 and to fulfill the legislative mandate under 8 U.S.C. 1103, 1226 and 1252. Such authority has been delegated to EOIR by 8 CFR part 1003.

Purpose(s):

Information in this system serves as the official record of immigration proceedings. EOIR employees use the information to prepare, process and track the proceedings. The information is further used to generate statistical reports and various documents, including hearing calendars and administrative orders.

Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses:

Information may be disseminated as follows:

(A) To the Department of State; the Department of Homeland Security; the Department of Health and Human Services; federal courts; the alien or alleged alien's representative attorney of record; and, to federal, state and local agencies. Information is disseminated to the Department of State, pursuant to 8 CFR 208.11, to allow its preparation of advisory opinions regarding applications for political asylum; to the Federal courts to enable review of EOIR administrative decisions on appeal; and, to the representative or attorney of record to ensure fair representation. Information is disseminated to the Department of Homeland Security as one of the parties affected by EOIR decisions, and as the agency which enforces the EOIR decision on a case. Information is disseminated to the Department of Health and Human Services as the provider of benefits to qualified immigrants, and as the custodian of some immigrants in immigration proceedings.

(B) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record.

(C) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute

unwarranted invasion of personal privacy.

(D) To the National Archives and Records Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(E) Where a record either on its face or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the records may be referred to the appropriate federal, state, local, foreign, or tribal, law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.

(F) In an appropriate proceeding before a court, or administrative or adjudicative body when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator holds the records to be relevant to the proceeding.

(G) Relevant information contained in this system of records may also be released to contractors, grantees, experts, consultants, students, and others performing or working under a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

(H) The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: Responding to an official inquiry by a state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Disclosure to Consumer Reporting Agencies:

Not applicable.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are maintained in file folders which are stored in file cabinets. A subset of records is maintained on fixed disks or removable disk packs which are stored in file cabinets. All records are stored in secured EOIR office space.

Retrievability:

Manual records are indexed by alien file number. Automated records are retrievable by a variety of identifying data elements including, but not limited to, alien file number, alien name and nationality, and attorney's or representative's name and UserId.

Safeguards:

Information maintained in the system is safeguarded in accordance with Department of Justice rules and procedures. Record files are maintained in file cabinets accessible only to EOIR employees. Automated information is stored on either fixed disks or removable disk packs which are stored in cabinets. Only EOIR employees in possession of specific codes and passwords will be able to generally access automated information. In addition, attorneys or authorized representatives will be able to access information specific to their case through the use of a secure UserId and password. All manual and automated records and mediums are located in EOIR office space accessible only to EOIR employees and locked during off-duty hours.

Retention and disposal:

Record files are retained for six months after the final disposition of the case, then forwarded to regional Federal Records Centers. Automated records are maintained in field office data bases for ninety days after final disposition, then transferred to the computer at EOIR headquarters and retained in accordance with the General Records Schedule filed with the National Archives and Records Administration.

System manager(s) and addresses:

General Counsel, Executive Office for Immigration Review, U.S. Department of Justice, 400 Leesburg Pike, Suite 2600, Falls Church, Virginia 22041.

Notification procedure:

Address all inquiries to the system manager listed above.

Record access procedures:

Portions of this system are exempt from disclosure and contest by 5 U.S.C. 522a (k)(2). Make all request for access to those portions not so exempted by writing to the system manager identified above. Clearly mark the envelope and letter "Privacy Access Requests" : provide the full name and notarized signature, or dated signature under oath of perjury, of the individual who is the subject of the record, his/her date and place of birth or any other identifying number or information which may assist in locating the record and a return address.

Contesting record procedures:

Direct all requests to contest or amend information maintained to the system manager identified above. Provide the information required under "Record Access Procedure." State clearly and concisely what information is being contested, the reason for contesting it, and the proposed amendment to the information.

Record source categories:

Department of Justice offices and employees, the Department of Homeland Security, the Department of State, the Department of Health and Human Services, and other federal and local agencies; and the parties to immigration proceedings, their attorneys or representatives, and their witnesses.

Exemptions claimed for the system:

The Attorney General has exempted certain records of this system from the access provisions of the Privacy Act (5 U.S.C. 552a(d)) pursuant to 5 U.S.C. 552a (k)(1) and (2). Rules have promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (d) and have been published in the Federal Register and are codified at 28 CFR 16.83 (a) and (b).

[\[TOP\]](#)

JUSTICE/EOIR-003

System name:

Practitioner Complaint/Disciplinary Files.

System location:

United States Department of Justice (DOJ), Executive Office for Immigration Review (EOIR), 5107 Leesburg Pike, Suite 2400, Falls Church, VA 22041; and at EOIR field offices as described in Justice/EOIR-999, most recently published April 13, 1999 at 64 FR 18051.

Categories of individuals covered by the system:

Attorneys and authorized representatives, as defined under 8 CFR 292.1, who have been subject to disciplinary complaints filed with, or received by, EOIR, including complaints from any source whatsoever; complaints who file complaints against such attorneys and authorized representatives.

Categories of records in the system:

The system contains the following categories of records: Complaints filed by any person or organization; records of state disciplinary authority proceedings; criminal conviction records; investigatory records, including preliminary inquiry reports; communications with individuals and/or outside agencies concerning disciplinary investigations and proceedings; interagency communications; copies of Notices of Intent to Discipline (NID) filed by EOIR and/or the Immigration and Naturalization Service (INS), together with supporting documentation; disciplinary proceeding transcripts; and settlement agreements and other dispositions, including administrative disciplinary decisions.

Authority for maintenance of the system:

Sec. 292 of the Immigration and Nationality Act, as amended at 8 U.S.C. 1362 and 8 CFR 292.3.

Purpose(s):

Information in the system is used by the office of the General Counsel, EOIR, in conducting disciplinary investigations and instituting disciplinary proceedings against immigration practitioners. The records are used in, and provide documentation of, among other things,

disciplinary investigations and formal proceedings instituted by EOIR. The information is further used to generate statistical reports and various administrative records, including printouts.

Routine uses of records maintained in the system, including categories of users and purpose of such uses:

EOIR may disclose relevant information as follows:

- (1) To Federal or state agencies as required by law;
- (2) In any proceeding before an adjudicative body before which DOJ, or any DOJ component or subdivision thereof, is authorized to appear and when any of the following is a party to litigation or has an interest in litigation and such records are determined by DOJ, or any component or subdivision thereof, to be arguably relevant to the litigation: DOJ or any DOJ components thereof; any DOJ employee in his/her official capacity; any DOJ employee in his/her individual capacity where DOJ has agreed to represent the employee; or the United States where DOJ, or any DOJ component thereof, determines that litigation is likely to involve or any of its subdivisions;
- (3) To an actual or potential party, including an immigration practitioner, or to his or her attorney of record, for the purpose of negotiation or discussion on such matters as settlement of a case or matter, conducting informal discovery proceedings involving records in this case or to otherwise ensure fair representation;
- (4) To complainants who file disciplinary complaints, or to their counsel of record;
- (5) To Federal, state, and local authorities, including, but not limited to, state bar grievance committees and other attorney discipline authorities for possible disbarment or disciplinary proceedings;
- (6) In any disciplinary complaint in which there is an indication of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, information, including investigatory information, may be disseminated to the appropriate agency (including any Federal, state, local, foreign, or tribal authority) charged with the responsibility of investigating or prosecuting such violation or with enforcing or implementing such law;

(7) To Members of Congress or their staff acting upon the Member's behalf where the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(8) To any Federal agency or to any individual or organization for the purpose of performing audit or oversight operations of DOJ and to meet related reporting requirements;

(9) To the new media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy; and

(10) To the National Archives and Records Administration (NARA) in records management inspections that may be conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records are maintained in file folders which are stored in filing cabinets. A subset of records are maintained on fixed magnetic disks or removable diskettes which are stored in filing cabinets. All records are stored in secured EOIR office space.

Retrievability:

Records are retrieved by name and/or docket number of the individual who is subject to disciplinary proceeding.

Safeguards:

Information maintained in the system is safeguarded in accordance with DOJ rules and procedures. Record files are maintained in file cabinets accessible only to EOIR employees. Automated information is stored on either fixed disks or removable diskette packs which are stored in filing cabinets or computers which may be accessed only through the use of passwords and/or name identifications issued to authorized EOIR employees. All manual and automated mediums are located in EOIR office space accessible only to EOIR employees and are locked during off-duty hours.

Retention and disposal:

Record files are maintained for six months after final disposition of the case, then forwarded to regional Federal Records Centers. Automated records are maintained at EOIR headquarters indefinitely.

System manager(s) and address:

Director, Executive Office for Immigration Review (EOIR), 5107 Leesburg Pike, Suite 2400, Arlington, VA 22204-6001, Falls Church, VA 22041.

Notification procedure:

Same as Records Access Procedures.

Record access procedures:

Portions of this system may be exempt from disclosure and contest pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). Any individual desiring to contest or amend information not subject to exemption must direct his/her request to the system manager noted above. In all cases, requests for access to a record shall be made in writing. Written requests may be submitted by mail or in person. Clearly mark the envelope and letter "Privacy Access Request" and provide the full name and notarized signature of the individual who is the subject of the record and any other identifying number or information that may assist in locating the record in accordance with 28 CFR 16.41(d), and a return address.

Contesting record procedure:

Direct all requests to contest or amend information maintained in the system to the system manager listed above in the manner described above in Records Access Procedures. Specify clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information.

Record source categories:

Law enforcement agencies, Federal and state courts, state bar licensing authorities, state grievance and/or disciplinary agencies, immigration practitioners' responses during disciplinary proceedings, and inquiries and/or complaints from witnesses or members of the general public including supporting documentation.

Systems exempted from certain provisions of the act:

The Attorney General has proposed to exempt certain records of this system from the automatic declassification provisions of the Privacy Act (5 U.S.C. 552a(d)), pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). Rules have been proposed in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e), and have been published as of this date in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/EOIR-999

System name: Appendix to Executive Office for Immigration Review System of Records

EOIR field offices are located as follows:

Executive Office for Immigration Review, Immigration Court, 901 N. Stuart Street, Suite 200
Arlington, VA 22203

Executive Office for Immigration Review, Immigration Court, Martin Luther King Jr. Federal
Bldg., 77 Forsyth Street, Room 112, Atlanta, GA 30303

Executive Office for Immigration Review, Immigration Court, US Appraisers Bldg., 103 S
Street, Room 702, Baltimore, MD 21202

Executive Office for Immigration Review, Immigration Court, 7850 Metro Parkway, Suite 200

Bloomington, MN 55425

Executive Office for Immigration Review, Immigration Court, JFK Federal Bldg., 15 New Sudbury Street, Room 320, Boston, MA 02203

Executive Office for Immigration Review, Immigration Court, 515 11th Street W., 3rd Floor, Bradenton, FL 34205

Executive Office for Immigration Review, Immigration Court, 130 Delaware Avenue, Suite 200, Buffalo, NY 14202

Executive Office for Immigration Review, Immigration Court, Federal Bldg., 55 E. Monroe Street, Suite 1900, Chicago, IL 60603

Executive Office for Immigration Review, Immigration Court, 1200 Main Street, Suite 700, Dallas, TX 75202.

Executive Office for Immigration Review, Immigration Court, Byron G. Rogers Federal Bldg., 1961 Stout Street, Room 1403, Denver, CO 80294

Executive Office for Immigration Review, Immigration Court, Brewery Park II, 1155 Brewster Blvd., Suite 450, Detroit, MI 48207

Executive Office for Immigration Review, Immigration Court, 625 Evans Street, Room 1401, Elizabeth, NJ 07201

Executive Office for Immigration Review, Immigration Court, 1545 Hawkins Blvd., Suite 200, El Paso, TX 79925

Federal Detention Center, 1705 E. Hanna Road, Suite 366, Eloy, AZ 85232

Executive Office for Immigration Review, Immigration Court, 3260 N. Pinal Parkway, Suite 200, Florence, AZ 85232

Executive Office for Immigration Review, Immigration Court, GSA Center, 651 Federal Drive, Suite 111-14, Guaynabo, San Juan, PR 00965

Executive Office for Immigration Review, Immigration Court, 201 E. Jackson Street, Harl
TX 78550

Executive Office for Immigration Review, Immigration Court, AA Ribicoff Federal Bldg. at
Courthouse, 450 Main Street, Room 509, Hartford, CT 06103–3015

Executive Office for Immigration Review, Immigration Court, PJKK Federal Bldg., 300 Al
Moanu Blvd., Room 8–112, Honolulu, HI 96850

Executive Office for Immigration Review, Immigration Court, 2320 La Branch Street, Roc
2235, Houston, TX 77004

Executive Office for Immigration Review, Immigration Court, 2409 La Brucherie Road, Irr
CA 92251

Krome North Processing Center, 18201 SW 12th Street, Miami, FL 33194

Laredo Service Processing Center, PO Box 440110, Laredo, TX 78044–0110

Executive Office for Immigration Review, Immigration Court, Mira Loma Facility, 45100 N
Street West, Lancaster, CA 93536

Executive Office for Immigration Review, Immigration Court, Pacific Enterprise Plaza, 33
Pepper Lane, Suite 200, Las Vegas, NV 89120

Executive Office for Immigration Review, Immigration Court, 606 S. Olive Street, Suite 14
Los Angeles, CA 90014

Port Isabel Processing Center, Route 3, Box 341, Bldg. 37, Los Fresnos, TX 78566

Executive Office for Immigration Review, Immigration Court, Clifton B. Davis Federal Bld
N. Main Street, Room 1026, Memphis, TN 38103

Executive Office for Immigration Review, Immigration Court, 155 S. Miami Avenue, Room
Miami, FL 33130

Ulster Correctional Facility, Berme Road, Napanoch, NY 12458

Executive Office for Immigration Review, Immigration Court, 970 Broad Street, Room 111
Newark, NJ 07102

Executive Office for Immigration Review, Immigration Court, One Canal Place, 365 Canal
Street, Suite 2450, New Orleans, LA 70130

Executive Office for Immigration Review, Immigration Court, 26 Federal Plaza, Suite 100
York, NY 10278

Executive Office for Immigration Review, Immigration Court, 1900 E. Whatley Road, Oak
LA 71463

Executive Office for Immigration Review, Immigration Court, 5449 South Semoran Blvd.,
200, Orlando, FL 32803

Executive Office for Immigration Review, Immigration Court, 1600 Callowhill Street, Room
Philadelphia, PA 19130

Executive Office for Immigration Review, Immigration Court, Federal Bldg., 200 E Mitche
Suite 200, Phoenix, AZ 85102

Executive Office for Immigration Review, Immigration Court, U.S. Post Office/Courthouse
615 E. Houston Street, Room 598, San Antonio, TX 78205-2040

Executive Office for Immigration Review, Immigration Court, 401 West A Street, Suite 80
Diego, CA 92101-7904

Executive Office for Immigration Review, Immigration Court, 550 Kearny Street, Suite 80
Francisco, CA 94108

INS San Pedro Service Processing Center, 2001 Seaside Avenue, Room 136, San Pedro
90731

Executive Office for Immigration Review, Immigration Court, Key Tower Bldg., 1000 Sec

Avenue, Suite 3150, Seattle, WA 98104

Executive Office for Immigration Review, Immigration Court, 160 N. Stone Avenue, Suite
Tucson, AZ 85701-1502

Executive Office for Immigration Review, Immigration Court, 201 Varick Street, Room 11
York, NY 10014

Executive Office for Immigration Review, Immigration Court, 3434 Concord Road, York, PA
17402

[\[TOP\]](#)

Federal Bureau of Investigation

JUSTICE/FBI-BRU

System name:

Blanket Routine Uses (BRU) Applicable to More Than One FBI Privacy Act System of Records

APPLICABILITY:

The following routine uses describe those types of disclosures which are common to more than one FBI Privacy Act system of records and which the FBI is establishing as "blanket" routine uses. Unless this or other published notice expressly provides otherwise, these blanket routine uses shall apply, without need of further implementation, to every existing FBI Privacy Act system of records and to all FBI systems of records created or modified hereafter. These blanket routine uses supplement but do not replace any routine uses that are separately published in the notices of individual record systems to which the blanket routine uses apply.

Routine uses of records maintained in the FBI, including categories of users and the purposes of such uses:

System records may be disclosed to the following persons or entities under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purpose for which the information was collected. (These routine uses are not meant to be

mutually exclusive and may overlap in some cases.)

BRU-1. Violations of Law, Regulation, Rule, Order, or Contract. If any system record, on face or in conjunction with other information, indicates a violation or potential violation of (whether civil or criminal), regulation, rule, order, or contract, the pertinent record may be disclosed to the appropriate entity (whether federal, state, local, joint, tribal, foreign, or international), that is charged with the responsibility of investigating, prosecuting, and/or enforcing such law, regulation, rule, order, or contract.

BRU-2. Non-FBI Employees. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function.

BRU-3. Appropriate Disclosures to the Public. To the news media or members of the general public in furtherance of a legitimate law enforcement or public safety function as determined by the FBI, e.g., to assist in locating fugitives; to provide notifications of arrests; to provide threat assessments, or similar information on potential threats to life, health, or property; or to inform the public appropriately informed of other law enforcement or FBI matters or other matters of legitimate public interest where disclosure could not reasonably be expected to constitute an unwarranted invasion of personal privacy. (The availability of information in pending criminal cases will be governed by the provisions of 28 CFR 50.2.)

BRU-4. Courts or Adjudicative Bodies. To a court or adjudicative body, in matters in which the FBI or any FBI employee in his or her official capacity, (b) any FBI employee in his or her individual capacity where the Department of Justice has agreed to represent the employee, (c) the United States, is or could be a party to the litigation, is likely to be affected by the litigation, or has an official interest in the litigation, and disclosure of system records has been determined by the FBI to be arguably relevant to the litigation. Similar disclosures may be made in analogous situations related to assistance provided to the Federal Government by non-FBI employees (see BRU-2).

BRU-5. Parties. To an actual or potential party or his or her attorney for the purpose of negotiating or discussing such matters as settlement of the case or matter, or informal discovery proceedings, in matters in which the FBI has an official interest and in which the FBI determines records in the system to be arguably relevant.

BRU-6. As Mandated by Law. To such recipients and under such circumstances and

procedures as are mandated by Federal statute or treaty.

BRU-7. Members of Congress. To a Member of Congress or a person on his or her staff on the Member's behalf when the request is made on behalf and at the request of the individual who is the subject of the record.

BRU-8. National Archives and Records Administration (NARA) Records Management. To the National Archives and Records Administration (NARA) for records management inspection and such other purposes conducted under the authority of 44 U.S.C. 2904 and 2906.

BRU-9. Auditors. To any agency, organization, or individual for the purposes of performing an authorized audit or oversight operations of the FBI and meeting related reporting requirements.

BRU-10. Former Employees. The DOJ may disclose relevant and necessary information to a former employee of the Department for purposes of: responding to an official inquiry by federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee if such communications may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility. (Such disclosures will be effected under procedures established in title 28, Code of Federal Regulations, sections 16.300-16.305 and DOJ Order 2710.8C, including any future revisions.)

BRU-11. The White House. To the White House (the President, Vice President, their staff, and other entities of the Executive Office of the President (EOP)), and, during Presidential transitions, the President-Elect and Vice-President Elect and their designees for appointment, employment, security, and access purposes compatible with the purposes for which the records were collected by the FBI, e.g., disclosure of information to assist the White House in making a determination whether an individual should be: (1) granted, denied, or permitted to continue in employment on the White House Staff; (2) given a Presidential appointment or Presidential recognition; (3) provided access, or continued access, to classified or sensitive information; or (4) permitted access, or continued access, to personnel or facilities of the White House/EOP complex. System records may be disclosed also to the White House and, during Presidential transitions, to the President Elect and Vice-President Elect and their designees for Executive Branch coordination of activities which relate to or have an effect upon the carrying out of the constitutional, statutory, or other official or ceremonial duties of the President, President Elect, Vice-President or Vice-President Elect.

BRU-12. Complainants and Victims. To complainants and/or victims to the extent deemed appropriate by the FBI to provide such persons with information and explanations concerning the progress and/or results of the investigations or cases arising from the matters of which they complained and/or of which they were victims.

BRU-13. To appropriate officials and employees of a federal agency or entity which require information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

BRU-14. To federal, state, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

BRU-15. To designated officers and employees of state, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor occupies or occupies a position of public trust as a law enforcement officer or detention officer or having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.

FBI RECORDS SYSTEMS TO WHICH THESE BLANKET ROUTINE USES DO NOT APPLY

These blanket routine uses shall not apply to the following FBI Privacy Act systems of records (to which shall apply only those routine uses established in the records system notice for each particular system):

JUSTICE/FBI-001, National Crime Information Center (NCIC).

JUSTICE/FBI-002, The FBI Central Records System.

JUSTICE/FBI-003, Bureau Mailing Lists.

JUSTICE/FBI-006, Electronic Surveillance (ELSUR) Indices.

JUSTICE/FBI-007, FBI Automated Payroll System.

JUSTICE/FBI-008, Bureau Personnel Management System (BPMS).

JUSTICE/FBI-009, Fingerprint Identification Records System (FIRS).

JUSTICE/FBI-010, Employee Travel Vouchers and Individual Earning Records.

JUSTICE/FBI-011, Employee Health Records.

JUSTICE/FBI-012, Time Utilization Record/Keeping (TURK) System.

JUSTICE/FBI-013, Security Access Control System (SACS).

JUSTICE/FBI-014, FBI Alcoholism Program.

JUSTICE/FBI-015, National Center for the Analysis of Violent Crime (NCAVC).

JUSTICE/FBI-016, FBI Counterdrug Information Indices System (CIIS).

JUSTICE/FBI-017, National DNA Index System (NDIS).

JUSTICE/FBI-018, National Instant Criminal Background Check System (NICS).

JUSTICE/FBI-019, Terrorist Screening Records System.

[\[TOP\]](#)

JUSTICE/FBI-001

System name:

National Crime Information Center (NCIC).

System location:

Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division, 1
Custer Hollow Road, Clarksburg, WV 26306.

Categories of individuals covered by the system:

A. Wanted Persons:

1. Individuals for whom federal warrants are outstanding.
2. Individuals who have committed or have been identified with an offense which is classified as a felony or serious misdemeanor under the existing penal statutes of the jurisdiction originating the entry and for whom a felony or misdemeanor warrant has been issued with respect to the offense which was the basis of the entry. Probation and parole violators meeting the following criteria.
3. A "Temporary Felony Want" may be entered when a law enforcement agency has neglected to take prompt action to establish a "want" entry for the apprehension of a person who has committed, or the officer has reasonable grounds to believe has committed, a felony and the person may seek refuge by fleeing across jurisdictional boundaries and circumstances preclude the immediate procurement of a felony warrant. A "Temporary Felony Want" shall be specifically identified as such and subject to verification and support by a proper warrant within 48 hours following the entry of a temporary want. The agency originating the "Temporary Felony Want" shall be responsible for subsequent verification or re-entry of a permanent want.
4. Juveniles who have been adjudicated delinquent and who have escaped or absconded from custody, even though no arrest warrants were issued. Juveniles who have been charged with the commission of a delinquent act that would be a crime if committed by an adult, and who have fled from the state where the act was committed.
5. Individuals who have committed or have been identified with an offense committed in a foreign country, which would be a felony if committed in the United States, and for whom a warrant of arrest is outstanding and for which an extradition treaty exists between the United States and that country.
6. Individuals who have committed or have been identified with an offense committed in Canada and for whom a Canada-Wide Warrant has been issued which meets the requirements of the warrant.

of the Canada-U.S. Extradition Treaty, 18 U.S.C. 3184.

B. Individuals who have been charged with serious and/or significant offenses:

1. Individuals who have been fingerprinted and whose criminal history record information has been obtained.
2. Violent Felons: Persons with three or more convictions for a violent felony or serious offense as defined by 18 U.S.C. 924(e).

C. Missing Persons:

1. A person of any age who is missing and who is under proven physical/mental disability, senile, thereby subjecting that person or others to personal and immediate danger.
2. A person of any age who is missing under circumstances indicating that the disappearance was not voluntary.
3. A person of any age who is missing under circumstances indicating that that person's physical safety may be in danger.
4. A person of any age who is missing after a catastrophe.
5. A person who is missing and declared unemancipated as defined by the laws of the person's state of residence and does not meet any of the entry criteria set forth in 1–4 above.

D. Individuals designed by the U.S. Secret Service as posing a potential danger to the President and/or other authorized protectees.

E. Members of Violent Criminal Gangs: Individuals about whom investigation has developed sufficient information to establish membership in a particular violent criminal gang by either:

1. Self admission at the time of arrest or incarceration, or
2. Any two of the following criteria:

- a. Identified as a gang member by a reliable informant;
- b. Identified as a gang member by an informant whose information has been corroborated;
- c. Frequents a gang's area, associates with known members, and/or affects gang dress, tattoos, or hand signals;
- d. Has been arrested multiple times with known gang members for offenses consistent with gang activity; or
- e. Self admission (other than at the time of arrest or incarceration).

F. Members of Terrorist Organizations: Individuals about whom investigation has developed sufficient information to establish membership in a particular terrorist organization using the same criteria listed above in paragraph E, items 1 and 2 a–e, as they apply to members of terrorist organizations rather than members of violent criminal gangs.

G. Unidentified Persons:

1. Any unidentified deceased person.
2. Any person who is living, but whose identity has not been ascertained (e.g., infant, air crash victim).
3. Any unidentified catastrophe victim.
4. Body parts when a body has been dismembered.

Categories of records in the system:

A. Stolen Vehicle File:

1. Stolen vehicles.
2. Vehicles wanted in conjunction with felonies or serious misdemeanors.

3. Stolen vehicle parts including certificates of origin or title.

B. Stolen License Plate File.

C. Stolen Boat File.

D. Stolen Gun File:

1. Stolen guns.

2. Recovered guns, when ownership of which has not been established.

E. Stolen Article File.

F. Securities File:

1. Serially numbered stolen, embezzled, or counterfeited securities.

2. "Securities" for present purposes of this file are currency (e.g., bills, bank notes) and documents or certificates which generally are considered to be evidence of debt (e.g., bonds, debentures, notes) or ownership of property (e.g., common stock, preferred stock), and documents which represent subscription rights, warrants and which are of the types traded on the securities exchanges in the United States, except for commodities futures. Also included are warehouse receipts, travelers checks and money orders.

G. Wanted Person File: Described in "Categories of individuals covered by the system: Wanted Persons, 1–4."

H. Foreign Fugitive File: Identification data regarding persons who are fugitives from foreign countries, who are described in "Categories of individuals covered by the system: A. Wanted Persons, 5 and 6."

I. Interstate Identification Index File: A cooperative federal-state program for the interstate exchange of criminal history record information for the purpose of facilitating the interstate exchange of such information among criminal justice agencies: Described in "Categories of individuals covered by the system: Interstate Identification Index, 7 and 8."

individuals covered by the system: B. 1."

J. Identification records regarding persons enrolled in the United States Marshals Service Witness Security Program who have been charged with serious and/or significant offenses. Described in "Categories of individuals covered by the system: B."

K. Bureau of Alcohol, Tobacco, and Firearms (BATF) Violent Felon File: Described in "Categories of individuals covered by the system: B.2."

L. Missing Person File: Described in "Categories of individuals covered by the system: C. Missing Persons."

M. U.S. Secret Service Protective File: Described in "Categories of individuals covered by the system: D."

N. Violent Criminal Gang File: A cooperative federal-state program for the interstate exchange of criminal gang information. For the purpose of this file, a "gang" is defined as a group of three or more persons with a common interest, bond, or activity characterized by criminal or delinquent conduct. Described in "Categories of individuals covered by the system: E. Members of Violent Criminal Gangs."

O. Terrorist File: A cooperative federal-state program for the exchange of information about terrorist organizations and individuals. For the purposes of this file, "terrorism" is defined as activities that involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state or would be a criminal violation if committed within the jurisdiction of the United States or any states, which appear to be intended to

1. Intimidate or coerce a civilian population,
2. Influence the policy of a government by intimidation or coercion, or
3. Affect the conduct of a government by crimes or kidnaping. Described in "Categories of individuals covered by the system: F. Members of Terrorist Organizations."

P. Unidentified Person File: Described in "Categories of individuals covered by the system: Unidentified Persons."

Authority for maintenance of the system:

The system is established and maintained in accordance with 28 U.S.C. 534; 28 CFR part 201; Department of Justice Appropriation Act, 1973, Pub. L. 92-544, 86 Stat. 1115; Securities Exchange Act of 1934, Pub. L. 73-411, 48 Stat. 1583; Securities Exchange Act of 1975, Pub. L. 94-29, 89 Stat. 97; and 18 U.S.C. 924 (e). Exec. Order No. 11888, 3 CFR (1974).

Purpose(s):

The purpose for maintaining the NCIC system of records is to provide a computerized database for ready access by a criminal justice agency making an inquiry and for prompt disclosure of information in the system from other criminal justice agencies about crimes and criminal records. This information assists authorized agencies in criminal justice objectives, such as apprehending fugitives, locating missing persons, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Data in NCIC files is exchanged with and for the official use of authorized officials of the government, the states, cities, penal and other institutions, and certain foreign governments. The data is exchanged most frequently, but not exclusively, through NCIC lines to federal criminal justice agencies, criminal justice agencies in the 50 states, the District of Columbia, Puerto Rico, U.S. Possessions, U.S. Territories, and certain authorized foreign and international criminal justice agencies. Criminal history data is disseminated to non-criminal justice agencies for use in connection with licensing for local/state employment or other purposes, but only where such dissemination is authorized by federal or state statute and approved by the Attorney General of the United States.

Data in NCIC files, other than the information described in "Categories of records in the system: I, J, K, M, N, and O" is disseminated to:

(1) A nongovernmental agency or subunit thereof which allocates a substantial part of its annual budget to the administration of criminal justice, whose regularly employed peace officers have full police powers pursuant to state law and have complied with the minimum

employment standards of governmentally employed police officers as specified by state statute;

(2) A noncriminal justice governmental department of motor vehicle or driver's license re established by a statute, which provides vehicle registration and driver record information to criminal justice agencies;

(3) A governmental regional dispatch center, established by a state statute, resolution, ordinance or Executive order, which provides communications services to criminal justice agencies; and

(4) The National Insurance Crime Bureau (NICB), a nongovernmental nonprofit agency acts as a national clearinghouse for information on stolen vehicles and offers free assistance to law enforcement agencies concerning automobile thefts, identification and recovery of stolen vehicles.

Disclosures of information from this system, as described in (1) through (4) above, are for the purpose of providing information to authorized agencies to facilitate the apprehension of fugitives, the location of missing persons, the location and/or return of stolen property, and other similar criminal justice objectives.

Information on missing children, missing adults who were reported missing while children, unidentified living and deceased persons may be disclosed to the National Center for Missing and Exploited Children (NCMEC). The NCMEC is a nongovernmental, nonprofit, federal funded corporation, serving as a national resource and technical assistance clearinghouse focusing on missing and exploited children. Information is disclosed to NCMEC to assist its efforts to provide technical assistance and education to parents and local governments regarding the problems of missing and exploited children, and to operate a nationwide missing children hotline to permit members of the public to telephone the Center from anywhere in the United States with information about a missing child.

System records may be disclosed to criminal justice agencies for the conduct of background checks under the National Instant Criminal Background Check System (NICS).

System records may be disclosed to noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies.

justice agencies.

System records may be disclosed to private contractors pursuant to a specific agreement with a criminal justice agency or a noncriminal justice governmental agency performing criminal justice dispatching functions or data processing/information services for criminal justice agencies to provide services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

In addition, information may be released to the news media and the public pursuant to 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

System records may be disclosed to a Member of Congress or staff acting on the member's behalf when the member or staff requests the information on behalf of and at the request of the individual who is the subject of the record; and,

System records may be disclosed to the National Archives and Records Administration or the General Services Administration for records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the NCIC system is stored electronically for use in a computer environment.

Retrievability:

On line access to data in NCIC is achieved by using the following search descriptors:

A. Stolen Vehicle File:

1. Vehicle identification number;
2. Owner applied number;
3. License plate number;
4. NCIC number (unique number assigned by NCIC computer to each NCIC record.)

B. Stolen License Plate File:

1. License plate number;
2. NCIC number.

C. Stolen Boat File:

1. Registration document number;
2. Hull serial number;
3. Owner applied number;
4. NCIC number.

D. Stolen Gun File:

1. Serial number of gun;

2. NCIC number.

E. Stolen Article File:

1. Serial number of article;

2. Owner applied number;

3. NCIC number.

F. Securities File:

1. Type, serial number, denomination of security, and issuer for other than U.S. Treasury issues and currency;

2. Type of security and name of owner of security;

3. Social Security number of owner of security (it is noted the requirements of the Privacy Act with regard to the solicitation of Social Security numbers have been brought to the attention of the members of the NCIC system);

4. NCIC number.

G. Wanted Person File:

1. Name and one of the following numerical identifiers:

- a. Date of birth;

- b. FBI number (number assigned by the Federal Bureau of Investigation to an arrest file record);

- c. Social Security number (it is noted the requirements of the Privacy Act with regard to

solicitation of Social Security numbers have been brought to the attention of the member of the NCIC system);

d. Operator's license number (driver's number);

e. Miscellaneous identifying number (military number or number assigned by federal, state or local authorities to an individual's record);

f. Originating agency case number;

2. Vehicle or license plate known to be in the possession of the wanted person;

3. NCIC number.

H. Foreign Fugitive File: See G, above.

I. Interstate Identification Index File:

1. Name, sex, race, and date of birth;

2. FBI number;

3. State identification number;

4. Social Security number;

5. Miscellaneous identifying number.

J. Witness Security Program File: See G, above.

K. BATF Violent Felon File: See G, above.

L. Missing Person file: See G, above, plus the age, sex, race, height and weight, eye and hair color of the missing person.

M. U.S. Secret Service Protective File: See G, above.

N. Violent Criminal Gang File: See G, above.

O. Terrorist File: See G, above.

P. Unidentified Person File: The age, sex, race, height and weight, eye and hair color of unidentified person.

Safeguards:

Data stored in the NCIC is documented criminal justice agency information and access data is restricted to duly authorized users. The following security measures are the minimum to be adopted by all authorized users having access to the NCIC.

Interstate Identification Index (III) File. These measures are designed to prevent unauthorized access to the system data and/or unauthorized use of data obtained from the computer file.

1. Computer Center.

a. The authorized user's computer site must have adequate physical security to protect any unauthorized personnel gaining access to the computer equipment or to any of the data.

b. Since personnel at these computer centers can have access to data stored in the system they must be screened thoroughly under the authority and supervision of an NCIC control terminal agency. (This authority and supervision may be delegated to responsible criminal justice agency personnel in the case of a satellite computer center being serviced through a state control terminal agency.) This screening will also apply to non-criminal justice maintenance or technical personnel.

c. All visitors to these computer centers must be accompanied by staff personnel at all times.

d. Computers having access to the NCIC must have the proper computer instructions and other built-in controls to prevent criminal history data from being accessible to any terminals other than authorized terminals.

e. Computers having access to the NCIC must maintain a record of all transactions against criminal history file in the same manner the NCIC computer logs all transactions. The NCIC identifies each specific agency entering or receiving information and maintains a record of those transactions. This transaction record must be monitored and reviewed on a regular basis to detect any possible misuse of criminal history data.

f. Each State Control terminal shall build its data system around a central computer, through which each inquiry must pass for screening and verification. The configuration and operation of the center shall provide for the integrity of the data base.

2. Communications:

a. Lines/channels being used to transmit criminal history information must be dedicated to criminal justice, i.e., there must be no terminals belonging to agencies outside the criminal justice system sharing these lines/channels.

b. Physical security of the lines/channels must be protected to guard against clandestine devices being utilized to intercept or inject system traffic.

3. Terminal Devices Having Access to NCIC:

a. All authorized users having terminal on this system must be required to physically place these terminals in secure locations within the authorized agency.

b. The authorized users having terminals with access to criminal history must screen terminal operators and restrict access to the terminal to a minimum number of authorized employees.

c. Copies of criminal history data obtained from terminal devices must be afforded security measures to prevent any unauthorized access to or use of the data.

d. All remote terminals on NCIS III will maintain a manual or automated log of computer criminal history inquiries with notations of individuals making requests for records for a minimum of one year.

Retention and disposal:

Unless otherwise removed, records will be retained in files as follows:

A. Vehicle File:

a. Unrecovered stolen vehicle records (including snowmobile records) which do not contain vehicle identification numbers (VIN) or Owner-applied number (OAN) therein, will be purged from file 90 days after date of entry. Unrecovered stolen vehicle records (including snowmobile records) which contain VINS or OANs will remain in file for the year of entry plus 4.

b. Unrecovered vehicles wanted in conjunction with a felony will remain in file for 90 days after entry. In the event a longer retention period is desired, the vehicle must be reentered.

c. Unrecovered stolen VIN plates, certificates of origin or title, and serially numbered stolen vehicle engines or transmissions will remain in file for the year of entry plus 4. (Job No. NC1-65-82-4, Part E. 13 h.(121A))

B. License Plate File: Unrecovered stolen license plates will remain in file for one year after the end of the plate's expiration year as shown in the record. (Job no. NC1-65-82-4, Part E. 13 h.(2)1A)

C. Boat file: Unrecovered stolen boat records, which contain a hull serial number or an OAN, will be retained in file for the balance of the year entered plus 4. Unrecovered stolen boat records which do not contain a hull serial number or an OAN will be purged from file 90 days after date of entry. (Job No. NC1-65-82-4, Part E. 13 h. (6))

D. Gun File:

a. Unrecovered weapons will be retained in file for an indefinite period until action is taken by the originating agency to clear the record.

b. Weapons entered in file as "recovered" weapons will remain in file for the balance of the year entered plus 2. (Job No. NC1-65-82-4, Part E. 13 h. (3))

E. Article File: Unrecovered stolen articles will be retained for the balance of the year entered plus one year. (Job No. NC1-65-82-4, Part E. 13 h. (4))

F. Securities File: Unrecovered stolen, embezzled or counterfeited securities will be retained for the balance of the year entered plus 4, except for travelers checks and money orders, which will be retained for the balance of the year entered plus 2. (Job No. NC1-65-82-4, Part E 13h. (5))

G. Wanted Person File: Person not located will remain in file indefinitely until action is taken by the originating agency to clear the record (except "Temporary Felony Wants" , which will be automatically removed from the file after 48 hours" . (Job No. NC1-65-87-114, Part E 13h. (7))

H. Foreign Fugitive File: Person not located will remain in file indefinitely until action is taken by the originating agency to clear the record.

I. Interstate Identification Index File: When an individual reaches age of 99. (Job No. NC1-65-95-03)

J. Witness Security Program File: Will remain in file until action is taken by the U.S. Marshals Service to clear or cancel the records.

K. BATF Violent Felon File: Will remain in file until action is taken by the BATF to clear or cancel the records.

L. Missing Persons File: Will remain in the file until the individual is located or action is taken by the originating agency to clear the record. (Job No. NC1-65-87-11, Part E 13h (8))

M.U.S. Secret Service Protective File: Will be retained until names are removed by the U.S. Secret Service.

N. Violent Criminal Gang File: Records will be subject to mandatory purge if inactive for five years.

O. Terrorist File: Records will be subject to mandatory purge if inactive for five years.

P. Unidentified Person File: Will be retained for the remainder of the year of entry plus 5 years.

System manager(s) and address:

Director, Federal Bureau of investigation, J. Edgar Hoover Building, 935 Pennsylvania Avenue NW., Washington, DC 20535-0001.

Notification procedure:

Same as the above.

Record access procedures:

It is noted the Attorney General has exempted this system from the access and contest procedures of the Privacy Act. However, the following alternative procedures are available to the requester. The procedures by which an individual may obtain a copy of his or her criminal history record from a state or local criminal justice agency are detailed in 28 CFR 20.34 appendix and are essentially as follows:

If an individual has a criminal record supported by fingerprints and that record has been entered in the III System, it is available to that individual for review, upon presentation of appropriate identification and in accordance with applicable state and federal administrative and statutory regulations.

Appropriate identification includes being fingerprinted for the purpose of insuring that the individual is who the individual purports to be. The record on file will then be verified through comparison of fingerprints.

Procedure:

1. All requests for review must be made by the subject of the record through a law enforcement agency which has access to the III System. That agency within statutory or regulatory limits can require additional identification to assist in securing a positive identification.
2. If the cooperating law enforcement agency can make an identification with fingerprint previously taken which are on file locally and if the FBI identification number of the individual record is available to that agency, it can make an on-line inquiry through NCIC to obtain the System record or, if it does not have suitable equipment to obtain an on-line response, it can obtain the record from Clarksburg, West Virginia, by mail. The individual will then be afforded the opportunity to review the record.

opportunity to see that record.

3. Should the cooperating law enforcement agency not have the individual's fingerprints locally, it is necessary for that agency to relate the prints to an existing record by having identification prints compared with those already on file in the FBI, or, possibly, in the state central identification agency.

The procedures by which an individual may obtain a copy of his or her criminal history record from the FBI are set forth in 28 CFR 16.30–16.34.

Contesting record procedures:

The Attorney General has exempted this system from the contest procedures of the Privacy Act. Under the alternative procedures described above under "Record Access Procedures," the subject of the requested record shall request the appropriate arresting agency, court, or correctional agency to initiate action necessary to correct any stated inaccuracy in the subject record or provide the information needed to make the record complete. The subject of a record may also direct his/her challenge as to the accuracy or completeness of any entry on his record to the FBI, Criminal Justice Information Services (CJIS) Division, ATTN: SCU, Room 1000 Custer Hollow Road, Clarksburg, WV 26306. The FBI will then forward the challenge to the agency which submitted the data requesting that agency to verify or correct the challenged entry. Upon the receipt of an official communication directly from the agency which confirms the original information, the FBI CJIS Division will make any changes necessary in accordance with the information supplied by that agency.

Record source categories:

Information contained in the NCIC system is obtained from local, state, tribal, federal, foreign, and international criminal justice agencies.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsection (c)(3) and (4); (d); (e)(1) and (3); (e)(4)(G) and (H), (e)(8) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(1) and (k)(3). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 552(c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/FBI-002

System name:

The FBI Central Records System.

System location:

a. Federal Bureau of Investigation, J. Edgar Hoover Building, 10th and Pennsylvania Avenue NW, Washington DC 20535; b. 56 field divisions (see Appendix); c. 16 Legal Attache (see Appendix).

Categories of individuals covered by the system:

- a. Individuals who relate in any manner to official FBI investigations including, but not limited to, subjects, suspects, victims, witnesses, and close relatives and associates who are relevant to an investigation.
- b. Applicants for and current and former personnel of the FBI and persons related thereto who are considered relevant to an applicant investigation, personnel inquiry, or other personnel matters.
- c. Applicants for and appointees to sensitive positions in the United States Government and persons related thereto who are considered relevant to the investigation.
- d. Individuals who are the subject of unsolicited information, who offer unsolicited information, request assistance, and make inquiries concerning record material, including general correspondence, and contacts with other agencies, businesses, institutions, clubs; the press and the news media.
- e. Individuals associated with administrative operations or services including pertinent functions, contractors and pertinent persons related thereto. (All manner of information concerning individuals may be acquired in connection with and relating to the varied investigative responsibilities of the FBI which are further described in "CATEGORIES OF INFORMATION COVERED BY THE SYSTEM")

RECORDS IN THE SYSTEM." Depending on the nature and scope of the investigation information may include, among other things, personal habits and conduct, financial information, travel and organizational affiliation of individuals. The information collected a matter of record and placed in FBI files.)

Categories of records in the system:

The FBI Central Records Systems—The FBI utilizes a central records system of maintain investigative, personnel, applicant, administrative, and general files. This system consists one numerical sequence of subject matter files, an alphabetical index to the files, and a supporting abstract system to facilitate processing and accountability of all important material placed in files. This abstract system is both a textual and an automated capability for locating mail. Files kept in FBI field offices are also structured in the same manner, except they utilize an abstract system.

The 281 classifications used by the FBI in its basic filing system pertain primarily to Federal violations over which the FBI has investigative jurisdiction. However, included in the 281 classifications are personnel, applicant, and administrative matters to facilitate the overall scheme. These classifications are as follows (the word "obsolete" following the name of classification indicates the FBI is no longer initiating investigative cases in these matters although the material is retained for reference purposes):

1. Training Schools; National Academy Matters: FBI National Academy Applicants. Covers general information concerning the FBI National Academy, including background investigation of individual candidates.
2. Neutrality Matters. Title 18, United States Code, Sections 956 and 958-962; Title 22, United States Code, Sections 1934 and 401.
3. Overthrow or Destruction of the Government. Title 18, United States Code, Section 2385.
4. National Firearms Act, Federal Firearms Act; State Firearms Control Assistance Act; Unlawful Possession or Receipt of Firearms. Title 26, United States Code, Sections 580-586; Title 18, United States Code, Sections 921-928; Title 18, United States Code, Sections 1201-1203.
5. Income Tax. Covers violations of Federal income tax laws reported to the FBI. Compliance

are forwarded to the Commissioner of the Internal Revenue Service.

6. Interstate Transportation of Strikebreakers. Title 18, United States Code, Section 123

7. Kidnapping. Title 28, United States Code, Sections 1201 and 1202.

8. Migratory Bird Act. Title 18, United States Code, Section 43; Title 16, United States Code, Section 703 through 718.

9. Extortion. Title 18, United States Code, Sections 876, 877, 875, and 873.

10. Red Cross Act. Title 18, United States Code, Sections 706 and 917.

11. Tax (Other than Income). This classification covers complaints concerning violations of Internal Revenue law as they apply to other than alcohol, social security and income and profits taxes, which are forwarded to the Internal Revenue Service.

12. Narcotics. This classification covers complaints received by the FBI concerning alleged violations of Federal drug laws. Complaints are forwarded to the headquarters of the Drug Enforcement Administration (DEA), or the nearest district office of DEA.

13. Miscellaneous. Section 125, National Defense Act, Prostitution; Selling Whiskey Within Five Miles of An Army Camp, 1920 only. Subjects were alleged violators of abuse of U.S. flag, fraudulent enlistment, selling liquor and operating houses of prostitution within restricted bounds of military reservations. Violations of Section 13 of the Selective Service Act (Conscription Act) were enforced by the Department of Justice as a war emergency measure with the Bureau exercising jurisdiction in the detection and prosecution of cases within the purview of that Section.

14. Sedition. Title 18, United States Code, Sections 2387, 2388, and 2391.

15. Theft from Interstate Shipment. Title 18, United States Code, Section 859; Title 18, United States Code, Section 660; Title 18 United States Code, Section 2117.

16. Violations of Federal Injunction (obsolete). Consolidated into Classification 69, "Contempt of Court" .

17. Fraud Against the Government, Department of Veterans Affairs, Department of Veterans Affairs Matters. Title 18, United States Code, Section 287, 289, 290, 371, or 1001, and Title 18, United States Code, Sections 787(a), 787(b), 3405, 3501, and 3502.

18. May Act. Title 18, United States Code, Section 1384.

19. Censorship Matter (obsolete). Pub. L. 77th Congress.

20. Federal Grain Standards Act (obsolete) 1920 only. Subjects were alleged violators of contracts for sale. Shipment of Interstate Commerce, Section 5, U.S. Grain Standards Act.

21. Food and Drugs. This classification covers complaints received concerning alleged violations of the Food, Drug and Cosmetic Act; Tea Act; Import Milk Act; Caustic Poison and Filled Milk Act. These complaints are referred to the Commissioner of the Food and Administration of the field component of that Agency.

22. National Motor Vehicle Traffic Act, 1922–27 (obsolete). Subjects were possible violators of the National Motor Vehicle Theft Act, Automobiles seized by Prohibitions Agents.

23. Prohibition. This classification covers complaints received concerning bootlegging and other violations of the alcohol tax laws. Such complaints are referred to the Bureau of Alcohol, Tobacco and Firearms, Department of the Treasury, or field representatives of that Agency.

24. Profiteering 1920–42 (obsolete). Subjects are possible violators of the Lever Act—Profiteering in food and clothing or accused company was subject of file. Bureau conducted investigations to ascertain profits.

25. Selective Service Act; Selective Training and Service Act. Title 50, United States Code, Section 462; Title 50, United States Code, Section 459.

26. Interstate Transportation of Stolen Motor Vehicle; Interstate Transportation of Stolen Aircraft. Title 18, United States Code, Sections 2311 (in part), 2312, and 2313.

27. Patent Matter. Title 35, United States Code, Sections 104 and 105.

28. Copyright Matter. Title 17, United States Code, Sections 104 and 105.

29. Bank Fraud and Embezzlement. Title 18, United States Code, Sections 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000.

30. Interstate Quarantine Law, 1922–25 (obsolete). Subjects alleged violators of Act of February 15, 1893, as amended, regarding interstate travel of persons afflicted with infectious diseases. Cases also involved unlawful transportation of animals, Act of February 2, 1906. Referrals were made to Public Health Service and the Department of Agriculture.

31. White Slave Traffic Act. Title 18, United States Code, Section 2421–2424.

32. Identification (Fingerprint) Matters. This classification covers general information concerning identification (fingerprint) matters.

33. Uniform Crime Reporting. This classification covers general information concerning Uniform Crime Reports, a periodic compilation of statistics of criminal violations throughout the United States.

34. Violation of Lacey Act. 1922–43. (obsolete) Unlawful Transportation and shipment of birds and fur seal skins.

35. Civil Service. This classification covers complaints received by the FBI concerning Civil Service matters which are referred to the Office of Personnel Management in Washington and regional offices of that Agency.

36. Mail Fraud. Title 18, United States Code, Section 1341.

37. False Claims Against the Government. 1921–22 (obsolete). Subjects submitted claims for allotment, vocational training, compensation as veterans under the Sweet Bill. Letters were generally referred elsewhere (Veterans Bureau). Violators apprehended for violation of No. 1, War Risk Insurance Act.

38. Application for Pardon to Restore Civil Rights. 1921–35 (obsolete). Subjects alleged

obtained their naturalization papers by fraudulent means. Cases later referred to Immig and Naturalization Service.

39. Falsely Claiming Citizenship (obsolete). Title 18, United States Code, Sections 911 and 1015(a)(b).

40. Passport and Visa Matter. Title 18, United States Code, Sections 1451–1546.

41. Explosives (obsolete). Title 50, United States Code, Sections 121 through 144.

42. Deserter; Deserter, Harboring. Title 10, United States Code, Sections 808 and 885.

43. Illegal Wearing of Uniforms; False Advertising or Misuse of Names, Words, Emblem Insignia; Illegal Manufacturer, Use, Possession, or Sale of Emblems and Insignia; Illegal Manufacture, Possession, or Wearing of Civil Defense Insignia; Miscellaneous, Forging Using Forged Certificate of Discharge from Military or Naval Service; Miscellaneous, False Making or Forging Naval, Military, or Official Pass; Miscellaneous, Forging or Counterfeiting Seal of Department or Agency of the United States, Misuse of the Great Seal of the United States or of the Seals of the President or the Vice President of the United States; Unauthorized Use of "Johnny Horizon" Symbol; Unauthorized Use of Smokey Bear Symbol. Title 18, United States Code, Sections 702, 703, and 704; Title 18, United States Code, Sections 701, 702, and 710; Title 36, United States Code, Section 182; Title 50, Appendix, United States Code, Section 2284; Title 46, United States Code, Section 249; Title 18, United States Code, Sections 498, 499, 506, 709, 711, 711a, 712, 713, and 714; Title 12, United States Code, Section 1723a; Title 22, United States Code, Section 2518.

44. Civil Rights; Civil Rights, Election Laws, Voting Rights Act, 1965, Title 18, United States Code, Sections 241, 242, and 245; Title 42, United States Code, Section 1973; Title 18, United States Code, Section 243; Title 18, United States Code, Section 244, Civil Rights Act—Federally Protected Activities; Civil Rights Act—Overseas Citizens Voting Rights Act, 1975.

45. Crime on the High Seas (includes stowaways on boats and aircraft). Title 18, United States Code, Sections 7, 13, 1243, and 2199.

46. Fraud Against the Government (includes Department of Health, Education and Welfare)

Department of Labor (CETA), and Miscellaneous Government Agencies), Anti-Kickback Statute; Department Assistance Act of 1950; False Claims, Civil; Federal-Aid Road Act; and Zinc Act; Public Works and Economic Development Act of 1965; Renegotiation Act, Criminal; Renegotiation Act, Civil; Trade Expansion Act of 1962; Unemployment Compensation Statutes; Economic Opportunity Act, Title 50, United States Code, Section 1211 et seq.; 31, United States Code, Section 231; Title 41, United States Code, Section 119; Title 40 United States Code, Section 489.

47. Impersonation. Title 18, United States Code, Sections 912, 913, 915, and 916.

48. Postal. Violation (Except Mail Fraud). This classification covers inquiries concerning Postal Service and complaints pertaining to the theft of mail. Such complaints are either forwarded to the Postmaster General or the nearest Postal Inspector.

49. Bankruptcy Fraud. Title 18, United States Code, Sections 151–155.

50. Involuntary Servitude and Slavery. U.S. Constitution, 13th Amendment; Title 18, United States Code, Sections 1581–1588, 241, and 242.

51. Jury Panel Investigations. This classification covers jury panel investigations which are requested by the appropriate Assistant Attorney General as authorized by 28 U.S.C. 53 AG memorandum 781, dated November 9, 1972. These investigations can be conducted upon such request and consist of an indices and arrest check, and only in limited important trials where defendant could have influence over a juror.

52. Theft, Robbery, Embezzlement, Illegal Possession or Destruction of Government Property. Title 18, United States Code, Sections 641, 1024, 1660, 2112, and 2114. Interference With Government Communications, Title 18, United States Code, Section 1632.

53. Excess Profits on Wool. 1918 (obsolete). Subjects possible violators of Government of Wool Clip Act of 1918.

54. Customs Laws and Smuggling. This classification covers complaints received concerning smuggling and other matters involving importation and entry of merchandise into and the exportation of merchandise from the United States. Complaints are referred to the nearest district office of the U.S. Customs Service or the Commissioner of Customs, Washington.

55. Counterfeiting. This classification covers complaints received concerning alleged violations of counterfeiting of U.S. coins, notes, and other obligations and securities of the Government. These complaints are referred to either the Director, U.S. Secret Service, or the nearest office of that Agency.

56. Election Laws. Title 18, United States Code, Sections 241, 242, 245, and 591–607; Title 18, United States Code, Section 1973; Title 26, United States Code, Sections 9012 and 9042; Title 26, United States Code, Sections 431–437, 439, and 441.

57. War Labor Dispute Act (obsolete). Pub. L. 89—77th Congress.

58. Corruption of Federal Public Officials. Title 18, United States Code, Sections 201–205–211; Public Law 89–4 and 89–136.

59. World War Adjusted Compensation Act of 1924–44 (obsolete). Bureau of Investigation charged with the duty of investigating alleged violations of all sections of the World War Adjusted Compensation Act (Pub. L. 472, 69th Congress (H.R. 10277)) with the exception of Section 704.

60. Anti-Trust, Title 15, United States Code, Sections 1–7, 12–27, and 13.

61. Treason or Misprision of Treason. Title 18, United States Code, Sections 2381, 2382, 2390, 756, and 757.

62. Administrative Inquiries. Misconduct Investigations of Officers and Employees of the Department of Justice and Federal Judiciary; Census Matters (Title 13, United States Code, Sections 211–214, 221–224, 304, and 305) Domestic Police Cooperation; Eight-Hour-Day Act (Title 40, United States Code, Sections 321, 332, 325a, 326); Fair Credit Reporting Act (Title 15, United States Code, Sections 1681q and 1681r); Federal Cigarette Labeling and Advertising Act (Title 15, United States Code, Section 1333); Federal Judiciary Investigations; Kickback Act (Title 18, United States Code, Section 874); Lands Division Matter, other Violations and/or Matters; Civil Suits—Miscellaneous; Soldiers' and Sailors' Civil Relief Act of 1940 (Title 38, United States Code, Sections 510–590); Tariff Act of 1930 (Title 19, United States Code, Section 1304); Unreported Interstate Shipment of Cigarettes (Title 15, United States Code, Sections 375 and 376); Fair Labor Standards Act of 1938 (Wages and Hours Law) (Title 29, United States Code, Sections 201–219); Conspiracy (Title 18, United States Code, Sections 2381, 2382, 2390, 756, and 757).

Code, Section 371 (formerly Section 88, Title 18, United States Code); effective September 1948).

63. Miscellaneous—Nonsubversive. This classification concerns correspondence from the public which does not relate to matters within FBI jurisdiction.

64. Foreign Miscellaneous. This classification is a control file utilized as a repository for intelligence information of value identified by country. More specific categories are placed in classification 108–113.

65. Espionage. Attorney General Guidelines on Foreign Counterintelligence; Internal Security Act of 1950; Executive Order 11905.

66. Administrative Matters. This classification covers such items as supplies, automobile salary matters and vouchers.

67. Personnel Matters. This classification concerns background investigations of applicants for employment with the FBI and folders for current and former employees.

68. Alaskan matters (obsolete). This classification concerns FBI investigations in the Territory of Alaska prior to its becoming a State.

69. Contempt of Court. Title 18, United States Code, Sections 401, 402, 3285, 3691, 3692, 3693, 3694, 3695, 3696, 3697, 3698, 3699, 3700, 3701, 3702, 3703, 3704, 3705, 3706, 3707, 3708, 3709, 3710, 3711, 3712, 3713, 3714, 3715, 3716, 3717, 3718, 3719, 3720, 3721, 3722, 3723, 3724, 3725, 3726, 3727, 3728, 3729, 3730, 3731, 3732, 3733, 3734, 3735, 3736, 3737, 3738, 3739, 3740, 3741, 3742, 3743, 3744, 3745, 3746, 3747, 3748, 3749, 3750, 3751, 3752, 3753, 3754, 3755, 3756, 3757, 3758, 3759, 3760, 3761, 3762, 3763, 3764, 3765, 3766, 3767, 3768, 3769, 3770, 3771, 3772, 3773, 3774, 3775, 3776, 3777, 3778, 3779, 3780, 3781, 3782, 3783, 3784, 3785, 3786, 3787, 3788, 3789, 3790, 3791, 3792, 3793, 3794, 3795, 3796, 3797, 3798, 3799, 3800, 3801, 3802, 3803, 3804, 3805, 3806, 3807, 3808, 3809, 3810, 3811, 3812, 3813, 3814, 3815, 3816, 3817, 3818, 3819, 3820, 3821, 3822, 3823, 3824, 3825, 3826, 3827, 3828, 3829, 3830, 3831, 3832, 3833, 3834, 3835, 3836, 3837, 3838, 3839, 3840, 3841, 3842, 3843, 3844, 3845, 3846, 3847, 3848, 3849, 3850, 3851, 3852, 3853, 3854, 3855, 3856, 3857, 3858, 3859, 3860, 3861, 3862, 3863, 3864, 3865, 3866, 3867, 3868, 3869, 3870, 3871, 3872, 3873, 3874, 3875, 3876, 3877, 3878, 3879, 3880, 3881, 3882, 3883, 3884, 3885, 3886, 3887, 3888, 3889, 3890, 3891, 3892, 3893, 3894, 3895, 3896, 3897, 3898, 3899, 3900, 3901, 3902, 3903, 3904, 3905, 3906, 3907, 3908, 3909, 3910, 3911, 3912, 3913, 3914, 3915, 3916, 3917, 3918, 3919, 3920, 3921, 3922, 3923, 3924, 3925, 3926, 3927, 3928, 3929, 3930, 3931, 3932, 3933, 3934, 3935, 3936, 3937, 3938, 3939, 3940, 3941, 3942, 3943, 3944, 3945, 3946, 3947, 3948, 3949, 3950, 3951, 3952, 3953, 3954, 3955, 3956, 3957, 3958, 3959, 3960, 3961, 3962, 3963, 3964, 3965, 3966, 3967, 3968, 3969, 3970, 3971, 3972, 3973, 3974, 3975, 3976, 3977, 3978, 3979, 3980, 3981, 3982, 3983, 3984, 3985, 3986, 3987, 3988, 3989, 3990, 3991, 3992, 3993, 3994, 3995, 3996, 3997, 3998, 3999, 4000, 4001, 4002, 4003, 4004, 4005, 4006, 4007, 4008, 4009, 4010, 4011, 4012, 4013, 4014, 4015, 4016, 4017, 4018, 4019, 4020, 4021, 4022, 4023, 4024, 4025, 4026, 4027, 4028, 4029, 4030, 4031, 4032, 4033, 4034, 4035, 4036, 4037, 4038, 4039, 4040, 4041, 4042, 4043, 4044, 4045, 4046, 4047, 4048, 4049, 4050, 4051, 4052, 4053, 4054, 4055, 4056, 4057, 4058, 4059, 4060, 4061, 4062, 4063, 4064, 4065, 4066, 4067, 4068, 4069, 4070, 4071, 4072, 4073, 4074, 4075, 4076, 4077, 4078, 4079, 4080, 4081, 4082, 4083, 4084, 4085, 4086, 4087, 4088, 4089, 4090, 4091, 4092, 4093, 4094, 4095, 4096, 4097, 4098, 4099, 4100, 4101, 4102, 4103, 4104, 4105, 4106, 4107, 4108, 4109, 4110, 4111, 4112, 4113, 4114, 4115, 4116, 4117, 4118, 4119, 4120, 4121, 4122, 4123, 4124, 4125, 4126, 4127, 4128, 4129, 4130, 4131, 4132, 4133, 4134, 4135, 4136, 4137, 4138, 4139, 4140, 4141, 4142, 4143, 4144, 4145, 4146, 4147, 4148, 4149, 4150, 4151, 4152, 4153, 4154, 4155, 4156, 4157, 4158, 4159, 4160, 4161, 4162, 4163, 4164, 4165, 4166, 4167, 4168, 4169, 4170, 4171, 4172, 4173, 4174, 4175, 4176, 4177, 4178, 4179, 4180, 4181, 4182, 4183, 4184, 4185, 4186, 4187, 4188, 4189, 4190, 4191, 4192, 4193, 4194, 4195, 4196, 4197, 4198, 4199, 4200, 4201, 4202, 4203, 4204, 4205, 4206, 4207, 4208, 4209, 4210, 4211, 4212, 4213, 4214, 4215, 4216, 4217, 4218, 4219, 4220, 4221, 4222, 4223, 4224, 4225, 4226, 4227, 4228, 4229, 4230, 4231, 4232, 4233, 4234, 4235, 4236, 4237, 4238, 4239, 4240, 4241, 4242, 4243, 4244, 4245, 4246, 4247, 4248, 4249, 4250, 4251, 4252, 4253, 4254, 4255, 4256, 4257, 4258, 4259, 4260, 4261, 4262, 4263, 4264, 4265, 4266, 4267, 4268, 4269, 4270, 4271, 4272, 4273, 4274, 4275, 4276, 4277, 4278, 4279, 4280, 4281, 4282, 4283, 4284, 4285, 4286, 4287, 4288, 4289, 4290, 4291, 4292, 4293, 4294, 4295, 4296, 4297, 4298, 4299, 4300, 4301, 4302, 4303, 4304, 4305, 4306, 4307, 4308, 4309, 4310, 4311, 4312, 4313, 4314, 4315, 4316, 4317, 4318, 4319, 4320, 4321, 4322, 4323, 4324, 4325, 4326, 4327, 4328, 4329, 4330, 4331, 4332, 4333, 4334, 4335, 4336, 4337, 4338, 4339, 4340, 4341, 4342, 4343, 4344, 4345, 4346, 4347, 4348, 4349, 4350, 4351, 4352, 4353, 4354, 4355, 4356, 4357, 4358, 4359, 4360, 4361, 4362, 4363, 4364, 4365, 4366, 4367, 4368, 4369, 4370, 4371, 4372, 4373, 4374, 4375, 4376, 4377, 4378, 4379, 4380, 4381, 4382, 4383, 4384, 4385, 4386, 4387, 4388, 4389, 4390, 4391, 4392, 4393, 4394, 4395, 4396, 4397, 4398, 4399, 4400, 4401, 4402, 4403, 4404, 4405, 4406, 4407, 4408, 4409, 4410, 4411, 4412, 4413, 4414, 4415, 4416, 4417, 4418, 4419, 4420, 4421, 4422, 4423, 4424, 4425, 4426, 4427, 4428, 4429, 4430, 4431, 4432, 4433, 4434, 4435, 4436, 4437, 4438, 4439, 4440, 4441, 4442, 4443, 4444, 4445, 4446, 4447, 4448, 4449, 4450, 4451, 4452, 4453, 4454, 4455, 4456, 4457, 4458, 4459, 4460, 4461, 4462, 4463, 4464, 4465, 4466, 4467, 4468, 4469, 4470, 4471, 4472, 4473, 4474, 4475, 4476, 4477, 4478, 4479, 4480, 4481, 4482, 4483, 4484, 4485, 4486, 4487, 4488, 4489, 4490, 4491, 4492, 4493, 4494, 4495, 4496, 4497, 4498, 4499, 4500, 4501, 4502, 4503, 4504, 4505, 4506, 4507, 4508, 4509, 4510, 4511, 4512, 4513, 4514, 4515, 4516, 4517, 4518, 4519, 4520, 4521, 4522, 4523, 4524, 4525, 4526, 4527, 4528, 4529, 4530, 4531, 4532, 4533, 4534, 4535, 4536, 4537, 4538, 4539, 4540, 4541, 4542, 4543, 4544, 4545, 4546, 4547, 4548, 4549, 4550, 4551, 4552, 4553, 4554, 4555, 4556, 4557, 4558, 4559, 4560, 4561, 4562, 4563, 4564, 4565, 4566, 4567, 4568, 4569, 4570, 4571, 4572, 4573, 4574, 4575, 4576, 4577, 4578, 4579, 4580, 4581, 4582, 4583, 4584, 4585, 4586, 4587, 4588, 4589, 4590, 4591, 4592, 4593, 4594, 4595, 4596, 4597, 4598, 4599, 4600, 4601, 4602, 4603, 4604, 4605, 4606, 4607, 4608, 4609, 4610, 4611, 4612, 4613, 4614, 4615, 4616, 4617, 4618, 4619, 4620, 4621, 4622, 4623, 4624, 4625, 4626, 4627, 4628, 4629, 4630, 4631, 4632, 4633, 4634, 4635, 4636, 4637, 4638, 4639, 4640, 4641, 4642, 4643, 4644, 4645, 4646, 4647, 4648, 4649, 4650, 4651, 4652, 4653, 4654, 4655, 4656, 4657, 4658, 4659, 4660, 4661, 4662, 4663, 4664, 4665, 4666, 4667, 4668, 4669, 4670, 4671, 4672, 4673, 4674, 4675, 4676, 4677, 4678, 4679, 4680, 4681, 4682, 4683, 4684, 4685, 4686, 4687, 4688, 4689, 4690, 4691, 4692, 4693, 4694, 4695, 4696, 4697, 4698, 4699, 4700, 4701, 4702, 4703, 4704, 4705, 4706, 4707, 4708, 4709, 4710, 4711, 4712, 4713, 4714, 4715, 4716, 4717, 4718, 4719, 4720, 4721, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4736, 4737, 4738, 4739, 4740, 4741, 4742, 4743, 4744, 4745, 4746, 4747, 4748, 4749, 4750, 4751, 4752, 4753, 4754, 4755, 4756, 4757, 4758, 4759, 4760, 4761, 4762, 4763, 4764, 4765, 4766, 4767, 4768, 4769, 4770, 4771, 4772, 4773, 4774, 4775, 4776, 4777, 4778, 4779, 4780, 4781, 4782, 4783, 4784, 4785, 4786, 4787, 4788, 4789, 4790, 4791, 4792, 4793, 4794, 4795, 4796, 4797, 4798, 4799, 4800, 4801, 4802, 4803, 4804, 4805, 4806, 4807, 4808, 4809, 4810, 4811, 4812, 4813, 4814, 4815, 4816, 4817, 4818, 4819, 4820, 4821, 4822, 4823, 4824, 4825, 4826, 4827, 4828, 4829, 4830, 4831, 4832, 4833, 4834, 4835, 4836, 4837, 4838, 4839, 4840, 4841, 4842, 4843, 4844, 4845, 4846, 4847, 4848, 4849, 4850, 4851, 4852, 4853, 4854, 4855, 4856, 4857, 4858, 4859, 4860, 4861, 4862, 4863, 4864, 4865, 4866, 4867, 4868, 4869, 4870, 4871, 4872, 4873, 4874, 4875, 4876, 4877, 4878, 4879, 4880, 4881, 4882, 4883, 4884, 4885, 4886, 4887, 4888, 4889, 4890, 4891, 4892, 4893, 4894, 4895, 4896, 4897, 4898, 4899, 4900, 4901, 4902, 4903, 4904, 4905, 4906, 4907, 4908, 4909, 4910, 4911, 4912, 4913, 4914, 4915, 4916, 4917, 4918, 4919, 4920, 4921, 4922, 4923, 4924, 4925, 4926, 4927, 4928, 4929, 4930, 4931, 4932, 4933, 4934, 4935, 4936, 4937, 4938, 4939, 4940, 4941, 4942, 4943, 4944, 4945, 4946, 4947, 4948, 4949, 4950, 4951, 4952, 4953, 4954, 4955, 4956, 4957, 4958, 4959, 4960, 4961, 4962, 4963, 4964, 4965, 4966, 4967, 4968, 4969, 4970, 4971, 4972, 4973, 4974, 4975, 4976, 4977, 4978, 4979, 4980, 4981, 4982, 4983, 4984, 4985, 4986, 4987, 4988, 4989, 4990, 4991, 4992, 4993, 4994, 4995, 4996, 4997, 4998, 4999, 5000, 5001, 5002, 5003, 5004, 5005, 5006, 5007, 5008, 5009, 5010, 5011, 5012, 5013, 5014, 5015, 5016, 5017, 5018, 5019, 5020, 5021, 5022, 5023, 5024, 5025, 5026, 5027, 5028, 5029, 5030, 5031, 5032, 5033, 5034, 5035, 5036, 5037, 5038, 5039, 5040, 5041, 5042, 5043, 5044, 5045, 5046, 5047, 5048, 5049, 5050, 5051, 5052, 5053, 5054, 5055, 5056, 5057, 5058, 5059, 5060, 5061, 5062, 5063, 5064, 5065, 5066, 5067, 5068, 5069, 5070, 5071, 5072, 5073, 5074, 5075, 5076, 5077, 5078, 5079, 5080, 5081, 5082, 5083, 5084, 5085, 5086, 5087, 5088, 5089, 5090, 5091, 5092, 5093, 5094, 5095, 5096, 5097, 5098, 5099, 5100, 5101, 5102, 5103, 5104, 5105, 5106, 5107, 5108, 5109, 5110, 5111, 5112, 5113, 5114, 5115, 5116, 5117, 5118, 5119, 5120, 5121, 5122, 5123, 5124, 5125, 5126, 5127, 5128, 5129, 5130, 5131, 5132, 5133, 5134, 5135, 5136, 5137, 5138, 5139, 5140, 5141, 5142, 5143, 5144, 5145, 5146, 5147, 5148, 5149, 5150, 5151, 5152, 5153, 5154, 5155, 5156, 5157, 5158, 5159, 5160, 5161, 5162, 5163, 5164, 5165, 5166, 5167, 5168, 5169, 5170, 5171, 5172, 5173, 5174, 5175, 5176, 5177, 5178, 5179, 5180, 5181, 5182, 5183, 5184, 5185, 5186, 5187, 5188, 5189, 5190, 5191, 5192, 5193, 5194, 5195, 5196, 5197, 5198, 5199, 5200, 5201, 5202, 5203, 5204, 5205, 5206, 5207, 5208, 5209, 5210, 5211, 5212, 5213, 5214, 5215, 5216, 5217, 5218, 5219, 5220, 5221, 5222, 5223, 5224, 5225, 5226, 5227, 5228, 5229, 5230, 5231, 5232, 5233, 5234, 5235, 5236, 5237, 5238, 5239, 5240, 5241, 5242, 5243, 5244, 5245, 5246, 5247, 5248, 5249, 5250, 5251, 5252, 5253, 5254, 5255, 5256, 5257, 5258, 5259, 5260, 5261, 5262, 5263, 5264, 5265, 5266, 5267, 5268, 5269, 5270, 5271, 5272, 5273, 5274, 5275, 5276, 5277, 5278, 5279, 5280, 5281, 5282, 5283, 5284, 5285, 5286, 5287, 5288, 5289, 5290, 5291, 5292, 5293, 5294, 5295, 5296, 5297, 5298, 5299, 5300, 5301, 5302, 5303, 5304, 5305, 5306, 5307, 5308, 5309, 5310, 5311, 5312, 5313, 5314, 5315, 5316, 5317, 5318, 5319, 5320, 5321, 5322, 5323, 5324, 5325, 5326, 5327, 5328, 5329, 5330, 5331, 5332, 5333, 5334, 5335, 5336, 5337, 5338, 5339, 5340, 5341, 5342, 5343, 5344, 5345, 5346, 5347, 5348, 5349, 5350, 5351, 5352, 5353, 5354, 5355, 5356, 5357, 5358, 5359, 5360, 5361, 5362, 5363, 5364, 5365, 5366, 5367, 5368, 5369, 5370, 5371, 5372, 5373, 5374, 5375, 5376, 5377, 5378, 5379, 5380, 5381, 5382, 5383, 5384, 5385, 5386, 5387, 5388, 5389, 5390, 5391, 5392, 5393, 5394, 5395, 5396, 5397, 5398, 5399, 5400, 5401, 5402, 5403, 5404, 5405, 5406, 5407, 5408, 5409, 5410, 5411, 5412, 5413, 5414, 5415, 5416, 5417, 5418, 5419, 5420, 5421, 5422, 5423, 5424, 5425, 5426, 5427, 5428, 5429, 5430, 5431, 5432, 5433, 5434, 5435, 5436, 5437, 5438, 5439, 5440, 5441, 5442, 5443, 5444, 5445, 5446, 5447, 5448, 5449, 5450, 5451, 5452, 5453, 5454, 5455, 5456, 5457, 5458, 5459, 5460, 5461, 5462, 5463, 5464, 5465, 5466, 5467, 5468, 5469, 5470, 5471, 5472, 5473, 5474, 5475, 5476, 5477, 5478, 5479, 5480, 5481, 5482, 5483, 5484, 5485, 5486, 5487, 5488, 5489, 5490, 5491, 5492, 5493, 5494, 5495, 5496, 5497, 5498, 5499, 5500, 5501, 5502, 5503, 5504, 5505, 5506, 5507, 5508, 5509, 5510, 5511, 5512, 5513, 5514, 5515, 5516, 5517, 5518, 5519, 5520, 5521, 5522, 5523, 5524, 5525, 5526, 5527, 5528, 5529, 5530, 5531, 5532, 5533, 5534, 5535, 5536, 5537, 5538, 5539, 5540, 5541, 5542, 5543, 5544, 5545, 5546, 5547, 5548, 5549, 5550, 5551, 5552, 5553, 5554, 5555, 5556, 5557, 5558, 5559, 5560, 5561, 5562, 5563, 5564, 5565, 5566, 5567, 5568, 5569, 5570, 5571, 5572, 5573, 5574, 5575, 5576, 5577, 5578, 5579, 5580, 5581, 5582, 5583, 5584, 5585, 5586, 5587, 5588, 5589, 5590, 5591, 5592, 5593, 5594, 5595, 5596, 5597, 5598, 5599, 5600, 5601, 5602, 5603, 5604, 5605, 5606, 5607, 5608, 5609, 5610, 5611, 5612, 5613, 5614, 5615, 5616, 5617, 5618, 5619, 5620, 5621, 5622, 5623, 5624, 5625, 5626, 5627, 5628, 5629, 5630, 5631, 5632, 5633, 5634, 5635, 5636, 5637, 5638, 5639, 5640, 5641, 5642, 5643, 5644, 5645, 5646, 5647, 5648, 5649, 5650, 5651, 5652, 5653, 5654, 5655, 56

74. Perjury. Title 18, United States Code, Sections 1621, 1622, and 1623.

75. Bondsmen and Sureties. Title 18, United States Code, Section 1506.

76. Escaped Federal Prisoner. Escape and Rescue; Probation Violator, Parole Violator, Mandatory, Release Violator. Title 18, United States Code, Sections 751–757, 1072; Title 18, United States Code. Sections 3651–3656; and Title 18, United States Code. Sections 4202–4207, 5037, and 4161–4166.

77. Applicants (Special Inquiry, Departmental and Other Government Agencies, except having special classifications). This classification covers the background investigations conducted by the FBI in connection with the aforementioned positions.

78. Illegal Use of Government Transportation Requests. Title 18, United States Code, Sections 287, 495, 508, 641, 1001 and 1002.

79. Missing Persons. This classification covers the FBI's Identification Division's assistance in the locating of missing persons.

80. Laboratory Research Matters. At FBI Headquarters this classification is used for Laboratory research matters. In field office files this classification covers the FBI's public affairs matters and involves contact by the FBI with the general public, Federal and State agencies, the Armed Forces, Corporations, the news media and other outside organizations.

81. Gold Hoarding. 1933–45. (obsolete) Gold Hoarding investigations conducted in accordance with an Act of March 9, 1933 and Executive Order issued August 28, 1933. Bureau instructed by Department to conduct no further investigations in 1935 under the Gold Reserve Act of 1934. Thereafter, all correspondence referred to Secret Service.

82. War Risk Insurance (National Life Insurance (obsolete)). This classification covers investigations conducted by the FBI in connection with civil suits filed under this statute.

83. Court of Claims. This classification covers requests for investigations of cases pending before the Court of Claims from the Assistant Attorney General in charge of the Civil Division of the Department of Justice.

84. Reconstruction Finance Corporation Act (obsolete). Title 15, United States Code, Chapter 14.
85. Home Owner Loan Corporation (obsolete). This classification concerned complaints received by the FBI about alleged violations of the Home Owners Loan Act, which were referred to the Home Owners Loan Corporation. Title 12, United States Code, Section 1401.
86. Fraud Against the Government—Small Business Administration. Title 15, United States Code, Section 645; Title 18, United States Code, Sections 212, 213, 215, 216, 217, 657, 1006, 1011, 1013, 1014, 1906, 1907, and 1909.
87. Interstate Transportation of Stolen Property (Heavy Equipment—Commercialized Theft). Title 18, United States Code, Sections 2311, 2314, 2315 and 2318.
88. Unlawful Flight to Avoid Prosecution, Custody, or Confinement; Unlawful Flight to Avoid Giving Testimony. Title 18, United States Code, Sections 1073 and 1074.
89. Assaulting or Killing a Federal Officer, Crimes Against Family Members, Congressional Assassination Statute, Title 18, United States Code, Sections 1111, 1114, 2232.
90. Irregularities in Federal Penal Institutions. Title 18, United States Code, Sections 1791 and 1792.
91. Bank Burglary, Bank Larceny; Bank Robbery. Title 18, United States Code, Section 2113.
92. Racketeer Enterprise Investigations. Title 18, United States Code. Section 3237.
93. Ascertaining Financial Ability. This classification concerns requests by the Department of Justice for the FBI to ascertain a person's ability to pay a claim, fine or judgment obtained against him by the United States Government.
94. Research matters. This classification concerns all general correspondence of the FBI with private individuals which does not involve any substantive violation of Federal law.
95. Laboratory Cases (Examination of Evidence in Other Than Bureau's Cases). The

classification concerns non-FBI cases where a duly constituted State, county or a municipal law enforcement agency in a criminal matter has requested an examination of evidence FBI Laboratory.

96. Alien Applicant (obsolete). Title 10, United States Code, Section 310.

97. Foreign Agents Registration Act. Title 18, United States Code, Section 951; Title 22, States Code, Sections 611–621; Title 50, United States Code, Sections 851–857.

98. Sabotage. Title 18, United States Code, Sections 2151–2156; Title 50, United States Section 797.

99. Plant Survey (obsolete). This classification covers a program wherein the FBI inspect industrial plants for the purpose of making suggestions to the operations of those plants to prevent espionage and sabotage.

100. Domestic Security. This classification covers investigations by the FBI in the domestic security field, e.g., Smith Act violations.

101. Hatch Act (obsolete). Public Law 252, 76th Congress.

102. Voorhis Act, Title 18, United States Code, Section 1386.

103. Interstate Transportation of Stolen Livestock, Title 18, United States Code, Sections 2311, 2316 and 2317.

104. Servicemen's Dependents Allowance Act of 1942 (obsolete). Public Law 625, 77th Congress, Sections 115–119.

105. Foreign Counterintelligence Matters. Attorney General Guidelines on Foreign Counterintelligence. Executive Order 11905.

106. Alien Enemy Control; Escaped Prisoners of War and Internees, 1944–55 (obsolete). Suspects were generally suspected escaped prisoners of war, members of foreign organizations, failed to register under the Alien Registration Act. Cases ordered closed by Attorney General after alien enemies returned to their respective countries upon termination.

hostilities.

107. Denaturalization Proceedings (obsolete). This classification covers investigation concerning allegations that an individual fraudulently swore allegiance to the United States in some other manner illegally obtained citizenship to the U.S. Title 8, United States Code, Section 738.

108. Foreign Travel Control (obsolete). This classification concerns security-type investigations wherein the subject is involved in foreign travel.

109. Foreign Political Matters. This classification is a control file utilized as a repository for intelligence information concerning foreign political matters broken down by country.

110. Foreign Economic Matters. This classification is a control file utilized as a repository for intelligence information concerning foreign economic matters broken down by country.

111. Foreign Social Conditions. This classification is a control file utilized as a repository for intelligence information concerning foreign social conditions broken down by country.

112. Foreign Funds. This classification is a control file utilized as a repository for intelligence information concerning foreign funds broken down by country.

113. Foreign Military and Naval Matters. This classification is a control file utilized as a repository for intelligence information concerning foreign military and naval matters broken down by country.

114. Alien Property Custodian Matter (obsolete). Title 50, United States Code, Sections 3146–3152. This classification covers investigations concerning ownership and control of property subject to claims and litigation under this statute.

115. Bond Default; Bail Jumper. Title 18, United States Code, Sections 3146–3152.

116. Department of Energy Applicant; Department of Energy, Employee. This classification concerns background investigations conducted in connection with employment with the Department of Energy.

117. Department of Energy, Criminal. Title 42, United States Code, Sections 2011–2281 Law 93–438.

118. Applicant, Intelligence Agency (obsolete). This classification covers applicant background investigations conducted of persons under consideration for employment by the Central Intelligence Group.

119. Federal Regulation of Lobbying Act. Title 2, United States Code, sections 261–270.

120. Federal Tort Claims Act, Title 28, United States Code, Sections 2671 to 2680. Investigations are conducted pursuant to specific request from the Department of Justice in connection with cases in which the Department of Justice represents agencies sued under the Act.

121. Loyalty of Government Employees (obsolete). Executive Order 9835.

122. Labor Management Relations Act, 1947. Title 29, United States Code, Sections 1601–176–178 and 186.

123. Section inquiry, State Department, Voice of America (U.S. Information Center) (Public Law 402, 80th Congress) (obsolete). This classification covers loyalty and security investigation of personnel employed by or under consideration for employment for Voice of America.

124. European Recovery Program Administration, formerly Foreign Operations Administration or E.R.P., European Recovery Programs; A.I.D. for International Development (obsolete). This classification covers security and loyalty investigation of personnel employed by or under consideration for employment with the European Recovery Program, Public Law 472, 80th Congress.

125. Railway Labor Act; Railway Labor Act—Employer's Liability Act Title 45, United States Code, Sections 151–163 and 181–188.

126. National Security Resources Board, Special Inquiry (obsolete). This classification covers loyalty investigations on employees and applicants of the National Security Resources Board.

127. Sensitive Positions in the United States Government, Public Law 266 (obsolete). This classification covers

Law 81st Congress.

128. International Development Program (Foreign Operations Administration) (obsolete) classification covers background investigations conducted on individuals who are to be assigned to duties under the International Development Program.

129. Evacuation Claims (obsolete). Public Law 886, 80th Congress.

130. Special Inquiry. Armed Forces Security Act (obsolete). This classification covers applicant-type investigations conducted for the Armed Forces security agencies.

131. Admiralty Matter. Title 46, United States Code, Sections 741–752 and 781–799.

132. Special Inquiry, Office of Defense Mobilization (obsolete). This classification covers applicant-type investigations of individuals associated with the Office of Defense Mobilization.

133. National Science Foundation Act, Applicant (obsolete). Public Law 507, 81st Congress.

134. Foreign Counterintelligence Assets. This classification concerns individuals who provide information to the FBI concerning Foreign Counterintelligence matters.

135. PROSAB (Protection of Strategic Air Command Bases of the U.S. Air Force) (obsolete). This classification covered contacts with individuals with the aim to develop information to protect bases of the Strategic Air Command.

136. American Legion Contact (obsolete). This classification covered liaison contracts with American Legion offices.

137. Informants. Other than Foreign Counterintelligence Assets. This classification concerns individuals who furnish information to the FBI concerning criminal violations on a continuing and confidential basis.

138. Loyalty of Employees of the United Nations and Other Public International Organizations. This classification concerns FBI investigations based on referrals from the Office of Personnel Management wherein a question or allegation has been received regarding the applicant's loyalty to the U.S. Government as described in Executive Order 10422.

139. Interception of Communications (Formerly, Unauthorized Publication or Use of Communications). Title 47, United States Code, Section 605; Title 47, United States Code, Section 501; Title 18, United States Code, Sections 2510–2513.

140. Security of Government Employees; Fraud Against the Government, Executive Order 10450.

141. False Entries in Records of Interstate Carriers. Title 47, United States Code, Section 20; Title 49, United States Code, Section 20.

142. Illegal Use of Railroad Pass. Title 49, United States Code, Section 1.

143. Interstate Transport of Gambling Devices. Title 15, United States Code, Sections 1170 through 1180.

144. Interstate Transportation of Lottery Tickets. Title 18, United States Code, Section 1170.

145. Interstate Transportation of Obscene Materials. Title 18, United States Code, Sections 1462, 1464, and 1465.

146. Interstate Transportation of Prison-Made Goods. Title 18, United States Code, Sections 1761 and 1762.

147. Fraud Against the Government—Department of Housing and Urban Development, Matters. Title 18, United States Code, Sections 657, 709, 1006, and 1010; Title 12, United States Code, Sections 1709 and 1715.

148. Interstate Transportation of Fireworks. Title 18, United States Code, Section 836.

149. Destruction of Aircraft or Motor Vehicles. Title 18, United States Code, Section 31—1.

150. Harboring of Federal Fugitives, Statistics (obsolete).

151. (Referral cases received from the Office of Personnel Management under Pub. L. 85-624; Agency for International Development; Department of Energy; National Aeronautics and

Administration; National Science Foundation; Peace Corps; Action; U.S. Arms Control and Disarmament Agency; World Health Organization; International Labor Organization; International Communications Agency. This classification covers referrals from the Office of Personnel Management where an allegation has been received regarding an applicant's access to the U.S. Government. These referrals refer to applicants from Peace Corps; Department of Energy, National Aeronautics and Space Administration, Nuclear Regulatory Commission, United States Arms Control and Disarmament Agency and the International Communications Agency.

152. Switchblade Knife Act. Title 15, United States Code, Sections 1241–1244.

153. Automobile Information Disclosure Act. Title 15, United States Code, Sections 1231

154. Interstate Transportation of Unsafe Refrigerators. Title 15, United States Code, Sections 1211–1214.

155. National Aeronautics and Space Act of 1958. Title 18, United States Code, Section

156. Employee Retirement Income Security Act. Title 29, United States Code, Sections 1021–1029, 1111, 1131, and 1141; Title 18, United States Code, Sections 644, 1027, and

157. Civil Unrest. This classification concerns FBI responsibility for reporting information on disturbances or demonstrations. The FBI's investigative responsibility is based on the Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Foreign Interest which became effective April 5, 1976.

158. Labor-Management Reporting and Disclosure Act of 1959 (Security Matter) (obsolete). Public Law 86–257, Section 504.

159. Labor-Management Reporting and Disclosure Act of 1959 (Investigative Matter). Title 18, United States Code, Sections 501, 504, 522, and 530.

160. Federal Train Wreck Statute. Title 18, United States Code, Section 1992.

161. Special Inquiries for White House, Congressional Committee and Other Government Agencies. This classification covers investigations requested by the White House.

Congressional committees or other Government agencies.

162. Interstate Gambling Activities. This classification covers information acquired concerning the nature and scope of illegal gambling activities in each field office.

163. Foreign Police Cooperation. This classification covers requests by foreign police for FBI to render investigative assistance to such agencies.

164. Crime Aboard Aircraft. Title 49, United States Code, Sections 1472 and 1473.

165. Interstate Transmission of Wagering Information. Title 18, United States Code, Section 1065.

166. Interstate Transportation in Aid of Racketeering. Title 18, United States Code, Section 1952.

167. Destruction of Interstate Property. Title 15, United States Code, Sections 1281 and

168. Interstate Transportation of Wagering Paraphernalia. Title 18, United States Code, 1953.

169. Hydraulic Brake Fluid Act (obsolete); 76 Stat. 437, Public Law 87–637.

170. Extremist Informants (obsolete). This classification concerns individuals who provide information on a continuing basis on various extremist elements.

171. Motor Vehicle Seat Belt Act (obsolete). Pub. L. 88–201, 80th Congress.

172. Sports Bribery. Title 18, United States Code, Section 244.

173. Public Accommodations. Civil Rights Act of 1964 Public Facilities; Civil Rights Act of 1964 Public Education; Civil Rights Act of 1964 Employment; Civil Rights Act of 1964. Title 42 United States Code, Section 2000; Title 18, United States Code, Section 245.

174. Explosives and Incendiary Devices; Bomb Threats (Formerly Bombing Matters; Bombing Matters, Threats). Title 18, United States Code, Section 844.

175. Assaulting, Kidnapping or Killing the President (or Vice President) of the United States. Title 18, United States Code, Section 1751.

176. Anti-riot Laws. Title 18, United States Code, Section 245.

177. Discrimination in Housing. Title 42, United States Code, Sections 3601–3619 and 3620.

178. Interstate Obscene or Harassing Telephone Calls. Title 47, United States Code, Section 223.

179. Extortionate Credit Transactions. Title 18, United States Code, Sections 891–896.

180. Desecration of the Flag. Title 18, United States Code, Section 700.

181. Consumer Credit Protection Act. Title 15, United States Code, Section 1611.

182. Illegal Gambling Business: Illegal Gambling Business, Obstruction; Illegal Gambling Business Forfeiture. Title 18, United States Code, Section 1955; Title 18, United States Code, Section 1511.

183. Racketeer, Influence and Corrupt Organizations. Title 18, United States Code, Sections 1961–1968.

184. Police Killings. This classification concerns investigations conducted by the FBI upon written request from local Chief of Police or duly constituted head of the local agency to actively participate in the investigation of the killing of a police officer. These investigations are based on a Presidential Directive dated June 3, 1971.

185. Protection of Foreign Officials and Official Guests of the United States. Title 18, United States Code, Sections 112, 970, 1116, 1117, and 1201.

186. Real Estate Settlement Procedures Act of 1974. Title 12, United States Code, Section 2602; Title 12, United States Code, Section 2606, and Title 12, United States Code, Section 2607.

187. Privacy Act of 1974, Criminal. Title 5, United States Code, Section 552a.

188. Crime Resistance. This classification covers FBI efforts to develop new or improved approaches, techniques, systems, equipment and devices to improve and strengthen law enforcement as mandated by the Omnibus Crime Control and Safe Streets Act of 1968.

189. Equal Credit Opportunity Act. Title 15, United States Code, Section 1691.

190. Freedom of Information/Privacy Acts. This classification covers the creation of a correspondence file to preserve and maintain accurate records concerning the handling of requests for records submitted pursuant to the Freedom of Information—Privacy Acts.

191. False Identity Matters. (obsolete) This classification covers the FBI's study and examination of criminal elements' efforts to create false identities.

192. Hobbs Act—Financial Institutions; Commercial Institutions Armored Carrier. Title 18, United States Code, Section 1951.

193. Hobbs Act—Commercial Institutions (obsolete). Title 18, United States Code, Section 1951; Title 47, United States Code, Section 506.

194. Hobbs Act—Corruption of Public Officials. Title 18, United States Code, Section 1951.

195. Hobbs Act—Labor Related. Title 18, United States Code, Section 1951.

196. Fraud by Wire. Title 18, United States Code, Section 1343.

197. Civil Actions or Claims Against the Government. This classification covers all civil suits involving FBI matters and most administrative claims filed under the Federal Tort Claims Act arising from FBI activities.

198. Crime on Indian Reservations. Title 18, United States Code, Sections 1151, 1152, and 1153.

199. Foreign Counterintelligence—Terrorism. Attorney General Guidelines on Foreign

Counterintelligence. Executive Order 11905.

200. Foreign Counterintelligence Matters. Attorney General Guidelines on Foreign Counterintelligence. Executive Order 11905.

201. Foreign Counterintelligence Matters. Attorney General Guidelines on Foreign Counterintelligence. Executive Order 11905.

202. Foreign Counterintelligence Matters. Attorney General Guidelines on Foreign Counterintelligence. Executive Order 11905.

203. Foreign Counterintelligence Matters. Attorney General Guidelines on Foreign Counterintelligence. Executive Order 11905.

204. Federal Revenue Sharing. This classification covers FBI investigations conducted under the Federal Revenue Sharing Act. The Attorney General has been authorized to bring civil action whenever he has reason to believe that a pattern or practice of discrimination in disbursement of funds under the Federal Revenue Sharing status exists.

205. Foreign Corrupt Practices Act of 1977. Title 15, United States Code, Section 78.

206. Fraud Against the Government—Department of Defense, Department of Agriculture, Department of Commerce, Community Services Organization, Department of Transportation. (See classification 46 (supra) for a statutory authority for this and the four following classifications.)

207. Fraud Against the Government—Environmental Protection Agency, National Aeronautics and Space Administration, Department of Energy, Department of Transportation.

208. Fraud Against the Government—General Services Administration.

209. Fraud Against the Government—Department of Health and Human Services (Formerly Department of Health, Education, and Welfare).

210. Fraud Against the Government—Department of Labor.

211. Ethics in Government Act of 1978, Title VI (Title 28, Sections 591–596).

212. Foreign Counterintelligence—Intelligence Community Support. This is an administrative classification for the FBI's operational and technical support to other Intelligence Community agencies.

213. Fraud Against the Government—Department of Education.

214. Civil Rights of Institutionalized Persons Act (Title 42, United States Code, Section 1

215. Foreign Counterintelligence Matters. Attorney General Guidelines on Foreign Counterintelligence. Executive Order 11905.

216. thru 229. Foreign Counterintelligence Matters. (Same authority as 215.)

230. thru 240. FBI Training Matters.

241. DEA Applicant Investigations.

242. Automation Matters.

243. Intelligence Identities Protection Act of 1982.

244. Hostage Rescue Team.

245. Drug Investigative Task Force.

246 thru 248. Foreign Counterintelligence Matters. (Same authority as 215.)

249. Environmental Crimes—Investigations involving toxic or hazardous waste violations

250. Tampering With Consumer Products (Title 18, U.S. Code, Section 1395).

251. Controlled Substance— Robbery;—Burglary (Title 18, U.S. Code, section 2118).

252. Violent Crime Apprehension Program (VICAP). Case folders containing records related to the VICAP Program, in conjunction with the National Center for the Analysis of Violent Crime Record System at the FBI Academy; Quantico, Virginia.

253. False Identification Crime Control Act of 1982 (Title 18, U.S. Code, Section 1028—Identity Theft and Related Activity in Connection With Identification Documents, and Section 1738—Unauthorized Use of Private Identification Documents Without a Disclaimer).

254. Destruction of Energy Facilities (Title 18, U.S. Code, Section 1365) relates to the destruction of property of nonnuclear energy facilities.

255. Counterfeiting of State and Corporate Securities (Title 18, U.S. Code, Section 511) covers the counterfeiting and forgery of all forms of what is loosely interpreted as securities.

256. Hostage Taking—Terrorism (Title 18, U.S. Code, Section 1203) prohibits taking of hostage(s) to compel third party to do or refrain from doing any act.

257. Trademark Counterfeiting Act (Title 18, United States Code, section 2320) covers the trafficking in goods which bear a counterfeited trademark.

258. Credit Card Fraud Act of 1984 (Title 18, United States Code, section 1029) covers the use of credit and related activities in connection with access devices (credit and debit cards).

259. Security Clearance Investigations Program. (Same authority as 215.)

260. Industrial Security Program. (Same authority as 215.)

261. Security Officer Matters. (Same authority as 215.)

262. Overseas Homicide (Attempted Homicide—International Terrorism). Title 18, United States Code, Section 2331.

263. Office of Professional Responsibility Matters.

264. Computer Fraud and Abuse Act of 1986. Electronic Communications Privacy Act of 1986.

- Title 18, United States Code, Section 1030; Title 18, United States Code, Section 2701.
265. Acts of Terrorism in the United States—International Terrorist. (Followed by predicate offense from other classification.)
266. Acts of Terrorism in the United States—Domestic Terrorist. (Followed by predicate from other classification.)
267. Drug-Related Homicide. Title 21, U.S. Code, Section 848(e).
268. Engineering Technical Matters—FCI.
269. Engineering Technical Matters—Non-FCI.
270. Cooperative Witnesses.
271. Foreign Counterintelligence Matters. Attorney General Guidelines on Foreign Counterintelligence. Executive Order 11905.
272. Money Laundering. Title 18, U.S. Code, Sections 1956 and 1957.
273. Adoptive Forfeiture Matter—Drug. Forfeiture based on seizure of property by state, or other Federal authority.
274. Adoptive Forfeiture Matter—Organized Crime. (Same explanation as 273.)
275. Adoptive Forfeiture Matter—White Collar Crime. (Same explanation as 273.)
276. Adoptive Forfeiture Matter—Violent Crime/Major Offenders Program. (Same explanation as 273.)
277. Adoptive Forfeiture Matter—Counterterrorism Program. (Same explanation as 273.)
278. Presidents Intelligence Oversight Board. Executive Order 12334.
279. Biological Weapons Anti-Terrorism Act of 1989. (Title 18, U.S. Code, Sections 175-

280. Equal Employment Opportunity Investigations.

281. Organized Crime Drug Investigations. Records Maintained in FBI Field Divisions—All divisions maintain for limited periods of time investigative, administrative and correspondence records, including files, index cards and related material, some of which are duplicated and reports and similar documents forwarded to FBI Headquarters. Most investigative activities conducted by FBI field divisions are reported to FBI Headquarters at one or more stages of investigation. There are, however, investigative activities wherein no reporting was made to Headquarters, e.g., pending cases not as yet reported and cases which were closed in the field division for any of a number of reasons without reporting to FBI Headquarters.

Duplicate records and records which extract information reported in the main files are all in the various divisions of the FBI to assist them in their day-to-day operation. These records are lists of individuals which contain certain biographic data, including physical description and photograph. They may also contain information concerning activities of the individual as reported to FBIHQ by the various field offices. The establishment of these lists is necessary by the needs of the Division to have immediate access to pertinent information duplicated in the data found in the central records without the delay caused by a time-consuming manual search of central indices. The manner of segregating these individuals varies depending on the particular needs of the FBI Division. The information pertaining to individuals who are on the list is derivative of information contained in the Central Records System. These duplicate records fall into the following categories:

- (1) Listings of individuals used to assist in the location and apprehension of individuals for whom legal process is outstanding (fugitives):
- (2) Listings of individuals used in the identification of particular offenders in cases where FBI has jurisdiction. These listings include various photograph albums and background information concerning persons who have been formerly charged with a particular crime and who are suspected in similar criminal activities; and photographs of individuals who are unknown but suspected of involvement in a particular criminal activity, for example, bank surveillance photographs:
- (3) Listings of individuals as part of an overall criminal intelligence effort by the FBI. This includes photograph albums, lists of individuals known to be involved in criminal activity, including theft from interstate shipment, interstate transportation of stolen property, and

individuals in the upper echelon of organized crime:

(4) Listings of individuals in connection with the FBI's mandate to carry out Presidential directives on January 8, 1943, July 24, 1950, December 15, 1953, and February 18, 1971, which designated the FBI to carry out investigative work in matters relating to espionage, sabotage, and foreign counterintelligence. These listings may include photograph album and other listings containing biographic data regarding individuals. This would include lists of identified and suspected foreign intelligence agents and informants:

(5) Special indices duplicative of the central indices used to access the Central Records System have been created from time to time in conjunction with the administration and investigation of major cases. This duplication and segregation facilitates access to documents prepared in connection with major cases.

In recent years, as the emphasis on the investigation of white collar crime, organized crime, and hostile foreign intelligence operations has increased, the FBI has been confronted with increasingly complicated cases, which require more intricate information processing capabilities. Since these complicated investigations frequently involve massive volumes of evidence and other investigative information, the FBI uses its computers, when necessary, to collate, analyze, and retrieve investigative information in the most accurate and expeditious manner possible. It should be noted that this computerized investigative information, when extracted from the main files or other commercial or governmental sources, is only maintained as necessary to support the FBI's investigative activities. Information from these internal computerized subsystems of the "Central Records System" is not accessed by any other agency. All disclosures of computerized information are made in printed form or other appropriate format, in accordance with the routine uses which are set forth below and in compliance with applicable security requirements.

Records also are maintained on a temporary basis relevant to the FBI's domestic police cooperating program, where assistance in obtaining information is provided to state and police agencies. Also, personnel type information, dealing with such matters as attendance and production and accuracy requirements is maintained by some divisions.

(The following chart identifies various listings or indexes maintained by the FBI which have been or are being used by various divisions of the FBI in their day-to-day operations. This identifies the list by name, description and use, and where maintained, i.e., FBI Headquarters and/or Field Office. The number of field offices which maintain these indices is also indicated.)

The list indicates those indexes which are in current use (designated by the word "active") and those which are no longer being used, although maintained (designated by the word "inactive"). There are 27 separate indices which are classified in accordance with existing regulations and are not included in this list. The following indices are no longer being used by the FBI but are being maintained at FBIHQ pending receipt of authority to destroy: Black Panther Party Photo Index; Black United Front Index; Security Index; and Wounded Knee Album.)

1. Administrative Index (ADEX). Consists of cards with descriptive data on individuals who were subject to investigation in a national emergency because they were believed to constitute a potential or active threat to the internal security of the United States. When ADEX was established in 1971, it was made up of people who were formerly on the Security Index, Reserve Index, and Agitator Index. This index is maintained in two separate locations in FBI Headquarters. ADEX was discontinued in January 1978. This list is inactive at FBI Headquarters and 29 Field Offices.

2. Anonymous Letter File. Consists of photographs of anonymous communications and extortionate credit transactions, kidnapping, extortion and threatening letters. It is active at FBI Headquarters.

3. Associates of DEA Class I Narcotics Violators Listing. Consists of a computer listing of individuals whom DEA has identified as associates of Class I Narcotics Violators. It is active at FBI Headquarters and 56 Field Offices.

4. Background Investigation Index—Department of Justice. Consists of cards on persons who have been the subject of a full field investigation in connection with their consideration for employment in sensitive positions with Department of Justice, such as U.S. Attorney, Federal judges, or a high level Department position. It is active at FBI Headquarters.

5. Background Investigation Index—White House, Other Executive Agencies, and Congress. Consists of cards on persons who have been the subject of a full field investigation in connection with their consideration for employment in sensitive positions with the White House, Executive agencies (other than the Department of Justice) and the Congress. Active at FBI Headquarters.

6. Bank Fraud and Embezzlement Index. Consists of individuals who have been the subject of a "Bank Fraud and Embezzlement" investigation. This file is used as an investigative aid. It is active in one Field Office.

7. Bank Robbery Album. Consists of photos of bank robbers, burglars, and larceny sub some field offices it will also contain pictures obtained from local police departments of armed robbers and thus potential bank robbers. The index is used to develop investigat leads in bank robbery cases and may also be used to show to witnesses of bank robber is usually filed by race, height, and age. This index is also maintained in one resident a (a suboffice of a field office). Active in 47 Field Offices.

8. Bank Robbery Nickname Index. Consists of nicknames used by known bank robbers index cards on each would contain the real name and method of operation and are filed alphabetical order. Active in one Field Office.

9. Bank Robbery Note File. Consists of photographs of notes used in bank robberies in the suspect has been identified. This index is used to help solve robberies in which the has not been identified but a note was left. The role is compared with the index to try to the sentence structure and handwriting for the purpose of identifying possible suspects at FBI Headquarters.

10. Bank Robbery Suspect Index. Consists of a control file or index cards with photos, if available, of bank robbers or burglars. In some field offices these people may be part of robbery album. This index is generally maintained and used in the same manner as the robbery album. Active in 33 Field Offices.

11. Car Ring Case Photo Album. Consists of photos of subjects and suspects involved i large car theft ring investigation. It is used as an investigative aid. Active in one Field Of

12. Car Ring Case Photo Album and Index. Consists of photos of subjects and suspect involved in a large car theft ring investigation. The card index maintained in addition to t photo album contains the names and addresses appearing on fraudulent title histories i stolen vehicles. Most of these names appearing on these titles are fictitious. But the pho album and card indexes are used as an investigative aid. Active in one Field Office.

13. Car Ring Case Toll Call Index. Consists of cards with information on persons who subscribe to telephone numbers to which toll calls have been placed by the major subj a large car theft ring investigation. It is maintained numerically by telephone number. It to facilitate the development of probable cause for a court-approved wiretap. Active in tv Offices.

14. Car Ring Theft Working Index. Contains cards on individuals involved in car ring the on which the FBI Laboratory is doing examination work. Active at FBI Headquarters.

15. Cartage Album. Consists of photos with descriptive data of individuals who have been convicted of theft from interstate shipment or interstate transportation of stolen property there is a reason to believe they may request the offense. It is used in investigating the violations. Active in three Field Offices.

16. Channelizing Index. Consists of cards with the names and case file numbers of people are frequently mentioned in information reports. The index is used to facilitate the distribution or channeling of information reports to appropriate files. Active in nine Field Offices.

17. Check Circular File. Consists of fliers numerically in a control file on fugitives who are notorious fraudulent check passers and who are engaged in a continuing operation of passing checks. The fliers, which include the subject's name, photo, a summary of the subject's method of operation and other identifying data, are used to alert other FBI field offices and business establishments which may be the victims of bad checks.

18. Computerized Telephone Number File (CTNF) Intelligence. Consists of a computer file of telephone numbers (and) subscribers' names and addresses) utilized by subjects and certain individuals which come to the FBI's attention during major investigations. During subsequent investigations, telephone numbers, obtained through subpoena, are matched the telephone numbers on file to determine connections or associations. Active at FBI Headquarters.

19. Con Man Index. Consists of computerized names of individuals, along with company affiliation, who travel nationally and internationally while participating in large-dollar-value financial swindles. Active in four Field Offices.

20. Confidence Game (Flim Flam) Album. Consists of photos with descriptive information on individuals who have been arrested for confidence games and related activities. It is used for investigative aid. Active in one Field Office.

21. Copyright Matters Index. Consists of cards of individuals who are film collectors and titles. It is used as a reference in the investigation of copyright matters. Active in one Field Office.

22. Criminal Intelligence Index. Consists of cards with name and file number of individuals who have become the subject of an antiracketeering investigation. The index is used as a query to ascertain file numbers and the correct spelling of names. This index is active in two Field Offices and one Resident Agency.

23. Criminal Informant Index. Consists of cards containing identity and brief background information on all active and inactive informants furnishing information in the criminal area. Active at FBI Headquarters.

24. DEA Class 1 Narcotics Violators Listing. Consists of a computer listing of narcotic violators—persons known to manufacture, supply, or distribute large quantities of illicit drugs—along with background data. It is used by the FBI in their role of assisting DEA in disseminating intelligence data concerning illicit drug trafficking. This index is also maintained in two Resident Agencies.

25. Deserter Index. Contains cards with the names of individuals who are known military deserters. It is used as an investigative aid. Active in four Field Offices.

26. False Identities Index. Contains cards with the names of deceased individuals whose identification certificates have been obtained by other persons for possible false identification uses and the connection with which the FBI laboratory has been requested to perform examinations. Active at FBI Headquarters.

27. False Identities List. Consists of a listing of names of deceased individuals whose identification certificates have been obtained after the person's death, and thus whose names are possibly being used for false identification purposes. The listing is maintained as part of the FBI's program to find persons using false identities for illegal purposes. Inactive at 31 Field Offices.

28. False Identity Photo Album. Consists of names and photos of people who have been positively identified as using a false identification. This is used as an investigative aid in the FBI's investigation of false identities. Inactive in two Field Offices.

29. FBI/Inspector General (IG) Case Pointer System (FICPS). Consists of a computerized listing of individual names of organizations which are the subject of active and inactive federal investigations, along with the name of the agency conducting the investigation. Data is available to IG offices throughout the federal government to prevent duplication of investigations.

activity. Active at FBI Headquarters.

30. FBI Wanted Persons Index. Consists of cards on persons being sought on the basis of Federal warrants covering violations which fall under the jurisdiction of the FBI. It is used as a ready reference to identify those fugitives. Active at FBI Headquarters.

31. Foreign Counterintelligence (FCI). Consists of cards with identity background data on active and inactive operational and informational assets in the foreign counterintelligence program. It is used as a reference aid on the FCI Asset program. Active at FBI Headquarters.

32. Fraud Against the Government Index. Consists of individuals who have been the subject of a "fraud against the Government" investigation. It is used as an investigative aid. Active at FBI Field Office.

33. Fugitive Bank Robbers File. Consists of fliers on bank robbery fugitives filed sequentially in a control file. FBI Headquarters distributes to the field offices fliers on bank robbers in a status for 15 or more days to facilitate their location. Active at FBI Headquarters and in 49 Field Offices.

34. General Security Index. Contains cards on all persons that have been the subject of a security classification investigation by the FBI field office. These cards are used for general reference purposes. Active in one Field Office.

35. Hoodlum License Plate Index. Consists of cards with the license plate numbers and descriptive data on known hoodlums and cars observed in the vicinity of hoodlum homes. Used for quick identification of such person in the course of investigation. The one index that is not fully retrievable is maintained by a resident agency. Active in three Field Offices.

36. Identification Order Fugitive Flier File. Consists of fliers numerically in a control file. When immediate leads have been exhausted in fugitive investigations and a crime of considerable public interest has been committed, the fliers are given wide circulation among law enforcement agencies throughout the United States and are posted in post offices. They contain the fugitive's photograph, fingerprints, and description. Active at FBI Headquarters and in 49 Field Offices.

37. Informant Index. Consists of cards with the name, symbol numbers, and brief background

information on the following categories of active and inactive informants, top echelon criminal informants, security informants, criminal information, operational and informational assets, extremist informants (discontinued), plant informant—informants on and about certain national basis (discontinued), and potential criminal informants. Active in 56 Field Offices.

38. Informants in Other Field Offices, Index of. Consist of cards with names and/or symbols numbers of informants in other FBI field offices that are in a position to furnish information would also be included on the index card. Active in 15 Field Offices.

39. Interstate Transportation of Stolen Aircraft Photo Album. Consists of photos and descriptive data on individuals who are suspects known to have been involved in interstate transportation of stolen aircraft. It is used as an investigative aid. Active in one Field Office.

40. IRS Wanted List. Consists of one-page fliers from IRS on individuals with background information who are wanted by IRS for tax purposes. It is used in the identification of persons wanted by IRS. Active in 11 Field Offices.

41. Kidnapping Book. Consists of data, filed chronologically, on kidnappings that have occurred since the early fifties. The victims' names and the suspects, if known, would be listed with a brief description of the circumstances surrounding the kidnapping. The file is used as a reference aid in matching up prior methods of operation in unsolved kidnapping cases. Active at FBI Headquarters and inactive in four Field Offices.

42. Known Check Passers Album. Consists of photos with descriptive data of persons known to pass stolen, forged, or counterfeit checks. It is used as an investigative aid. Active in four Field Offices.

43. Known Gambler Index. Consists of cards with names, descriptive data, and sometimes photos of individuals who are known bookmakers and gamblers. The index is used in organized crime and gambling investigations. Subsequent to GAO's review, and at the recommendation of the inspection team at one of the two field offices where the index was destroyed and thus is not included in the total. Active in five Field Offices.

44. La Cosa Nostra (LCN) Membership Index. Contains cards on individuals having been identified as members of the LCN index. The cards contain personal data and pictures. The index is used solely by FBI agents for assistance in investigating organized crime matters.

Active at FBI Headquarters and 55 Field Offices.

45. Leased Line Letter Request Index. Contains cards on individuals and organizations or have been the subject of a national security electronic surveillance where a leased line was necessary. It is used as an administrative and statistical aid. Active at FBI Headquarters.

46. Mail Cover Index. Consists of cards containing a record of all mail covers conducted on individuals and groups since about January 1973. It is used for reference in preparing mail requests. Active at FBIHQ.

47. Military Deserter Index. Consists of cards containing the names of all military deserters where the various military branches have requested FBI assistance in locating. It is used as an administrative aid. Active at FBI Headquarters.

48. National Bank Robbery Album. Consists of fliers on bank robbery suspects held sequentially in a control file. When an identifiable bank camera photograph is available in a case has been under investigation for 30 days without identifying the subject, FBIHQ sends a flier to the field offices to help identify the subject. Active at FBI Headquarters and in 42 Field Offices.

49. National Fraudulent Check File. Contains photographs of the signature on stolen and counterfeit checks. It is filed alphabetically but there is no way of knowing the names are real or fictitious. The index is used to help solve stolen check cases by matching checks obtained from such cases against the index to identify a possible suspect. Active at FBI Headquarters.

50. National Security Electronic Surveillance Card File. Contains cards recording electronic surveillances previously authorized by the Attorney General and previously and currently authorized by the FISC; current and previous assets in the foreign counterintelligence file and a historical, inactive section which contains cards believed to record nonconsented physical entries in national security cases, previously toll billings, mail covers and lease agreements. The inactive section also contains cards Attorney General approvals and denials for warrantless electronic surveillance in the national security cases. Inactive at FBI Headquarters.

51. Night Depository Trap Index. Contains cards with the names of persons who have been involved in the theft of deposits made in bank night depository boxes. Since these thefts involved various methods, the FBI uses the index to solve such cases by matching up suspects.

methods to identify possible suspects. Active at FBI Headquarters.

52. Organized Crime Photo Album. Consists of photos and background information on individuals involved in organized crime activities. The index is used as a ready reference identifying organized crime figures within the field offices' jurisdiction. Active in 13 Field

53. Photospread Identification Elimination File. Consists of photos of individuals who have subjects and suspects in FBI investigations. It also includes photos received from other enforcement agencies. These pictures can be used to show witnesses of certain crimes in 14 Field Offices.

54. Prostitute Photo Album. Consists of photos with background data on prostitutes who prior local or Federal arrests for prostitution. It is used to identify prostitutes in connection investigations under the White Slave Traffic Act. Active in four Field Offices.

55. Royal Canadian Mounted Police (RCMP) Wanted Circular File. Consists of a control individuals with background information of persons wanted by the RCMP. It is used to notify the RCMP if an individual is located. Active in 17 Field Offices.

56. Security Informant Index. Consists of cards containing identity and brief background information on all active and inactive informants furnishing information in the criminal area. Active at FBI Headquarters.

57. Security Subjects Control Index. Consists of cards containing the names and case file numbers of individuals who have been subject to security investigations check. It is used as a reference source. Active in one Field Office.

58. Security Telephone Number Index. Contains cards with telephone subscriber information subpoenaed from the telephone company in any security investigation. It is maintained numerically by the last three digits in the telephone number. It is used for general reference purposes in security investigations. Active in one Field Office.

59. Selective Service Violators Index. Contains cards on individuals being sought on the basis of Federal warrants for violation of the Selective Service Act. Active at FBI Headquarters

60. Sources of Information Index. Consists of cards on individuals and organizations suspected

banks, motels, local government that are willing to furnish information to the FBI with sufficient frequency to justify listing for the benefit of all agents. It is maintained to facilitate the use of such sources. Active in 10 Field Offices.

61. Special Services Index. Contains cards of prominent individuals who are in a position to furnish assistance in connection with FBI investigative responsibility. Active in 28 Field Offices.

62. Stolen Checks and Fraud by Wire Index. Consists of cards on individuals involved in check and fraud by wire violations. It is used as an investigative aid. Active in one Field Office.

63. Stop Notices Index. Consists of cards on names of subjects or property where the field office has placed a stop at another law enforcement agency or private business such as shops in the event information comes to the attention of that agency concerning the subject or property. This is filed numerically by investigative classification. It is used to insure that the agency where the stop is placed is notified when the subject is apprehended or the property is located or recovered. Active in 43 Field Offices.

64. Surveillance Locator Index. Consists of cards with basic data on individuals and businesses which have come under physical surveillance in the city in which the field office is located. It is used for general reference purposes in antiracketeering investigations. Active in two Field Offices.

65. Telephone Number Index—Gamblers. Contains information on persons identified as a result of a subpoena for the names of subscribers to particular telephone numbers. The index cards are filed by the last three digits of the telephone number. The index is used in gambling investigations. Active in two Field Offices.

66. Telephone Subscriber and Toll Records Check Index. Contains cards with information on persons identified as the result of a formal request or subpoena to the phone company for the identity of subscribers to particular telephone numbers. The index cards are filed by telephone number and would also include identity of the subscriber, billing party's identity, subscriber's address, date of request from the telephone company, and file number. Active in one Field Office.

67. Thieves, Couriers and Fences Photo Index. Consists of photos and background information on individuals who are known to be thieves, couriers, or fences. Active in 10 Field Offices.

on individuals who are or are suspected of being thieves, couriers, or fences based on their past activity in the area of interstate transportation of stolen property. It is used as an investigative aid. Active in four Field Offices.

68. Toll Record Request Index. Contains cards on individuals and organizations on whose records have been obtained in national security related cases and with respect to which they had to prepare a request letter. It is used primarily to facilitate the handling of repeat requests on individuals listed. Active at FBIHQ.

69. Top Burglar Album. Consists of photos and background data of known and suspected burglars involved in the area of interstate transportation of stolen property. It is used as an investigative aid. Active in four Field Offices.

70. Top Echelon Criminal Informer Program (TECIP) Index. Consists of cards containing identity and brief background information on individuals who are either furnishing high level information in the organized crime area or are under development to furnish such information. The index is used primarily to evaluate, corroborate, and coordinate informant information to develop prosecutive data against racket figures under Federal, State, and local statutes. Active at FBI Headquarters.

71. Top Ten Program File. Consists of fliers, filed numerically in a control file, on fugitives considered by the FBI to be 1 of the 10 most wanted. Including a fugitive of the top 10 usually assures a greater national news coverage as well as nation-wide circulation of the flier. Active at FBI Headquarters and in 44 Field Offices.

72. Top Thief Program Index. Consists of cards of individuals who are professional burglar robbers, or fences dealing in items likely to be passed in interstate commerce or who travel interstate to commit the crime. Usually photographs and background information would be obtained on the index card. The index is used as an investigative aid. Active in 27 Field Offices.

73. Truck Hijack Photo Album. Contains photos and descriptive data of individuals who are suspected truck hijackers. It is used as an investigative aid and for displaying photos to witnesses and/or victims to identify unknown subjects in hijacking cases. Active in four Field Offices.

74. Truck Thief Suspect Photo Album. Consists of photos and background data on individuals

previously arrested or are currently suspects regarding vehicle theft. The index is used as an investigative aid. Active in one Field Office.

75. Traveling Criminal Photo Album. Consists of photos with identifying data of individuals convicted of various criminal offenses and may be suspects in other offenses. It is used as an investigative aid. Active in one Field Office.

76. Veterans Administrative (VA)/Federal Housing Administration (FHA) Matters Index. Consists of cards of individuals who have been subject of an investigation relative to VA and FHA matters. It is used as an investigative aid. Active in one Field Office.

77. Wanted Fliers File. Consists of fliers, filed numerically in a control file, on badly wanted fugitives whose apprehension may be facilitated by a flier. The flier contains the names, photographs, aliases, previous convictions, and a caution notice. Active at FBI Headquarters and in 46 Field Offices.

78. WheelDEX. Contains the nicknames and the case file numbers of organized crime members. It is used in organized crime investigations. Active in one Field Office.

79. White House Special Index. Contains cards on all potential White House appointees, members, guests, and visitors that have been referred to the FBI by the White House security office for a records check to identify any adverse or derogatory information. This index is used to expedite such check in view of the tight timeframe usually required. Active at FBI Headquarters.

80. Witness Protection Program Index. Contains cards on individuals who have been furnished a new identity by the U.S. Justice Department because of their testimony in organized crime trials. It is used primarily to notify the U.S. Marshals Service when information related to the safety of a protected witness comes to the FBI's attention. Active at FBI Headquarters.

Authority for maintenance of the system:

Federal Records Act of 1950, Title 44, United States Code, chapter 31, section 3101; and 36, Code of Federal Regulations, chapter XII, require Federal agencies to insure that accurate and proper records are made and preserved to document the organization, functions, policies, decisions, procedures and transactions and to protect the legal and financial rights of the Federal Government, title 28, United States Code, section 534, delegates authority to the

Attorney General to acquire, collect, classify, and preserve identification, criminal identification records, and other records.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records, both investigative and administrative, are maintained in this system in order to enable the FBI to function efficiently as an authorized, responsive component of the Department of Justice. Therefore, information in this system is disclosed to officials and employees of the Department of Justice, and/or all components thereof, who have need of the information for the performance of their official duties.

Personal information from this system may be disclosed as a routine use to any Federal agency where the purpose in making the disclosure is compatible with the law enforcement purpose for which it was collected, e.g., to assist the recipient agency in conducting a law enforcement or intelligence investigation, to assist the recipient agency in making a determination concerning an individual's suitability for employment and/or trustworthiness for employment and/or trustworthiness for access clearance purposes, or to assist the recipient agency in the performance of any authorized function where access to records in this system is declared by the recipient agency to be relevant to that function.

In addition, personal information may be disclosed from this system to members of the Executive Branch of the Federal Government in response to a specific request, or at the initiation of the FBI, where disclosure appears relevant to the authorized function of the recipient judicial or court system. An example would be where an individual is being considered for employment by a Federal judge. Information in this system may be disclosed as a routine use to any state or local government agency directly engaged in the criminal justice process, e.g., police, prosecution, penal, probation and parole, and the judiciary, where access is directly related to a law enforcement function of the recipient agency, e.g., in connection with a lawful criminal intelligence investigation, or making a determination concerning an individual's suitability for employment as a state or local law enforcement employee or concerning a victim's compensation under a state statute. Disclosure to a state or local government agency, (a) directly engaged in the criminal justice process or (b) for a licensing or regulatory function, is considered on an individual basis only under exceptional circumstances, as determined by the FBI.

Information in this system pertaining to the use, abuse or traffic of controlled substance

be disclosed as a routine use to federal, state or local law enforcement agencies and to licensing or regulatory agencies empowered to engage in the institution and prosecution cases before courts and licensing boards in matters relating to controlled substances, including courts and licensing boards responsible for the licensing or certification of individuals in the fields of pharmacy and medicine.

In any health care-related civil or criminal case, investigation, or matter, information indicating patient harm, neglect, or abuse, or poor or inadequate quality of care, at a health care facility or by a health care provider, may be disclosed as a routine use to any Federal, State, local, tribal, foreign, joint, international, or private entity that is responsible for regulating, licensing, registering, or accrediting any health care provider or health care facility, or enforcing any health care-related laws or regulations. Further, information indicating an ongoing quality of care problem by a health care provider or at a health care facility may be disclosed to the appropriate health plan. Additionally, unless otherwise prohibited by applicable law, information indicating patient harm, neglect, abuse, or poor or inadequate quality of care may be disclosed to the affected patient or his or her representative or guardian at the discretion and in the manner determined by the agency in possession of the information. Information in this system may be disclosed as a routine use in a proceeding before a court of adjudication, e.g., the Equal Employment Opportunity Commission and the Merit Systems Protection Board, before which the FBI is authorized to appear, when (a) the FBI or any employee in his or her official capacity, or (b) any employee in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (c) the United States, where the FBI determines it is likely to be affected by the litigation, is a party to litigation or has an interest in litigation and such records are determined by the FBI to be relevant to the litigation.

Information in this system may be disclosed as a routine use to an organization or individual in both the public or private sector if deemed necessary to elicit information or cooperation from the recipient for use by the FBI in the performance of an authorized activity. An example would be where the activities of an individual are disclosed to a member of the public in order to obtain his/her assistance in our apprehension or detection efforts.

Information in this system may be disclosed as a routine use to an organization or individual in both the public or private sector where there is reason to believe the recipient is or could become the target of a particular criminal activity or conspiracy, to the extent the information is relevant to the protection of life or property.

Information in this system may be disclosed to a legitimate agency of a foreign government

where the FBI determines that the information is relevant to that agency's responsibilities, where the dissemination serves the best interests of the U.S. Government, and where the purpose of making the disclosure is compatible with the purpose for which the information was collected.

Relevant information may be disclosed from this system to the news media and general public where there exists a legitimate public interest, e.g., to assist in the location of Federal fugitives, to provide notification of arrests, and where necessary for protection from imminent threat to life or property. This would include releases of information in accordance with 28 CFR 50.2.

A record relating to an actual or potential civil or criminal violation of the copyright statutes, Title 17, United States Code, or the trademark statutes, Titles 15 and 17, U.S. Code, may be disseminated to a person injured by such violation to assist him/her in the institution or maintenance of a suit brought under such titles. The FBI has received inquiries from private citizens and Congressional offices on behalf of constituents seeking assistance in locating individuals such as missing children and heirs to estates. Where the need is acute, and it appears FBI files may be the only lead in locating the individual, consideration will be given to furnishing relevant information to the requester. Information will be provided only in those instances where there are reasonable grounds to conclude from available information that the individual being sought would want the information to be furnished, e.g., an heir to a large estate. Information with regard to missing children will not be provided where they have reached their majority.

Information contained in this system, may be made available to a Member of Congress or acting upon the member's behalf when the member of staff requests the information in connection with and at the request of the individual who is the subject of the record.

A record from this system of records may be disclosed as a routine use to the National Archives and Records Administration and General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906, to the extent that the legislation governing the records permits.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance.

from the former employee regarding a matter within that person's former area of respon

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information relating to health care fraud may be disclosed to private health plans, or associations of private health plans, and health insurers, or associations of health insurers, for the following purposes: to promote the coordination of efforts to prevent, detect, investigate and prosecute health care fraud; to assist efforts by victims of health care fraud to obtain restitution; to enable private health plans to participate in local, regional, and national health care fraud task force activities; and to assist tribunals having jurisdiction over claims against private health plans.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

The active main files are maintained in hard copy form and some inactive records are maintained on microfilm. Investigative information which is maintained in computerized form may be stored in memory, on disk storage, on computer tape, or on a computer printed

Retrievability:

The FBI General Index must be searched to determine what information, if any, the FBI have in its files. Index records, or pointers to specific FBI files, are created on all manner of subject matters, but the predominant type record is the name index record. It should be noted that the FBI does not index all individuals who furnish information or all names developed during the course of an investigation. Only that information considered pertinent, relevant, or useful for future retrieval, is indexed. In certain major cases, individuals interviewed may be interviewed to facilitate the administration of the investigation. The FBI has automated that portion of its index containing the most recent information—15 years for criminal related matters and 30 years for intelligence and other type matters.

Automation will not change the "Central Records System" ; it will only facilitate more efficient and expeditious access to the main files. Searches against the automated records are accomplished on a "batch off-line" basis for certain submitting agencies where the name

search requests conform to FBI specified formats and also in an "on-line" mode with the video display terminals for other requests. The FBI will not permit any organization, public or private, outside the FBI to have direct access to the FBI indices system. All searches against the indices data base will be performed on site within FBI space by FBI personnel with the assistance of the automated procedures, where feasible. Automation of the various FBI office indices was completed in 1989. This automation initiative has been on a "day-one" basis. This indices system points to specific files within a given field office. Additionally, certain complicated investigative matters may be supported by specialized computer systems on individual microcomputers. Indices created in these environments are maintained as part of a particular computer system and accessible only through the system or through printed output of the indices. Full text retrieval is used in a limited number of cases as an investigative technique. It is not part of the normal search process and is not used as a substitute for the General Index or computer indices mentioned above.

The FBI will transfer historical records to the National Archives consistent with 44 U.S.C. 3401. No record of individuals or subject matter will be retained for transferred files; however, a record of the file numbers will be retained to provide full accountability of FBI files and to preserve the integrity of the filing system.

Safeguards:

Records are maintained in a restricted area and are accessed only by agency personnel. FBI employees receive a complete background investigation prior to being hired. All employees are cautioned about divulging confidential information or any information contained in FBI files. Failure to abide by this provision violates Department of Justice regulations and may violate certain statutes providing maximum severe penalties of a ten thousand dollar fine or 10 years imprisonment or both. Employees who resign or retire are also cautioned about divulging confidential information acquired in the jobs. Registered mail is used to transmit routine hard copy records between field offices. Highly classified records are hand carried by Special Agents or personnel of the Armed Forces Courier Service. Highly classified or sensitive privacy information, when electronically transmitted between field offices, is transmitted in encrypted form to prevent interception and interpretation. Information transmitted in teletype form is placed in the files of both the receiving and transmitting field offices. Field offices involved in certain complicated investigative matters may be provided with on-line access to the duplicative computerized information which is maintained for them on disk storage in the FBI Computer Center in Washington, DC, and this computerized data is also transmitted in encrypted

Retention and disposal:

As the result of an extensive review of FBI records conducted by NARA, records evaluated as historical and permanent will be transferred to the National Archives after established retention periods and administrative needs of the FBI have elapsed. As deemed necessary, certain records may be subject to restricted examination and usage, as provided by 44 U.S.C. § 2104.

FBI record disposition programs relevant to this System are conducted in accordance with the FBI Records Retention Plan and Disposition Schedule which was approved by the Archivist of the United States and the U.S. District Court, District of Columbia. Investigative, application, and administrative records which meet the destruction criteria will be destroyed after 20 or 30 years at FBI Headquarters and after 1, 5, 10 or 20 years in FBI Field Offices. Historical records will be transferred to the National Archives after 30 or 50 years, contingent upon investigative and administrative needs. The administrative indices and listings described within this System will be appraised separately and disposition authority established. (Job No. NC1-65-82-4 and amendments)

System manager(s) and address:

Director, Federal Bureau of Investigation, Washington, DC 20535.

Notification procedure:

Same as above.

Record access procedures:

A request for access to a record from the system shall be made in writing with the envelope clearly marked and the letter clearly marked "Privacy Access Request". Include in the request your full complete address, date of birth, place of birth, notarized signature, and other identifying information you may wish to furnish to assist in making a proper search of our records. Also include the general subject matter of the document or its file number. The requester will also provide a return address for transmitting the information. Requests for access to information maintained at FBI Headquarters must be addressed to the Director, Federal Bureau of Investigation, Washington, DC 20535. Requests for information maintained at FBI field divisions or Le

Attaches must be made separately and addressed to the specific field division or Legal listed in the appendix to this system notice.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should all direct their request to the Director, Federal Bureau of Investigation, Washington, DC 20535, stating clearly and concisely what information is being contested, the reasons for contesting, and the proposed amendment to the information sought.

Record source categories:

The FBI, by the very nature and requirement to investigate violations of law within its investigative jurisdiction and its responsibility for the internal security of the United States, collects information from a wide variety of sources. Basically, it is the result of investigative efforts and information furnished by other Government agencies, law enforcement agencies, and the general public, informants, witnesses, and public source material.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3), (d), (e) (1), (2) (3), (e)(4) (G) and (H), (e)(8) (f), (g), of the Privacy Act pursuant to 5 U.S.C. 552a (j) and Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (e).

**Appendix of Field Divisions and Legal Attaches for the Federal Bureau of Investigation
Field Divisions; Justice/FBI-999**

5th Floor, 445 Broadway, Albany, NY 12201.

POB 25186, Albuquerque, NM 87125.

POB 100560, Anchorage, AK 99510.

POB 1683, Atlanta, GA 30370.

7142 Ambassador Road, Baltimore, MD 21207.

2122 Building, Birmingham, AL 35203.

One Center Plaza, Suite 600, Boston, MA 02108.

111 West Huron Street, Buffalo, NY 14202.

6010 Kenley Lane, Charlotte, NC 28217.

219 S. Dearborn St., Chicago, IL 60604.

POB 1277, Cincinnati, OH 45201.

1240 E. 9th St., Cleveland, OH 44199.

POB 137, Columbia, SC 29202.

1801 W. Lamar, Dallas, TX 75202.

POB 1229, Denver, CO 80201.

POB 2118, Detroit, MI 48231.

700 E. San Antonio Ave., El Paso, TX 79901.

POB 50164, Honolulu, HI 96850.

POB 61369, Houston, TX 77208.

POB 1186, Indianapolis, IN 45206.

100 W. Capitol St., Jackson, MS 39269.

POB 8928, Jacksonville, FL 32239.

POB 2449, Kansas City, MO 64142.

POB 10368, Knoxville, TN 37919.

POB 16032, Las Vegas, NV 89101.

POB 21470, Little Rock, AR 72221-1470.

11000 Wilshire Blvd., Los Angeles, CA 90024.

POB 2467, Louisville, KY 40201.

167 N. Main St., Memphis, TN 38103.

POB 592418, Miami, FL 33159.

POB 2058, Milwaukee, WI 53201.

111 Washington Ave. South S-1100, Minneapolis, MN 55401.

POB 2128, Mobile, AL 36652.

POB 1158, Newark, NJ 07101.

POB 2058, New Haven, CT 06521.

POB 51930, New Orleans, LA 70151.

POB 1425, New York, NY 10008.

POB 3828, Norfolk, VA 23514.

POB 54511, Oklahoma City, OK 73154.

POB 548, Omaha, NE 68101.

600 Arch St., Philadelphia, PA 19106.

201 E. Indianola, Phoenix, AZ 85012.

POB 1315, Pittsburgh, PA 15230.

POB 709, Portland, OR 97207.

POB 12325, Richmond, VA 23241.

POB 13130, Sacramento, CA 95813.

POB 7251, St. Louis, MO 63177.

125 S. State St., Salt Lake City, UT 84138.

POB 1630, San Antonio, TX 78296.

880 Front St., San Diego, CA 92188.

POB 36015, San Francisco, CA 94102.

POB BT, San Juan, PR 00936.

915 2nd Ave., Seattle, WA 98174.

POB 3646, Springfield, IL 62708.

POB 172177, Tampa, FL 33602.

Washington Field Office, Washington, DC 20535.

Federal Bureau of Investigation Academy, Quantico, VA 22135.

Legal Attaches: (Send c/o the American Embassy for the Cities indicated).

Athens, Greece (PSC 108, Box 45, APO AE 09842) Bangkok, Thailand (Box 67, APO F 96546).

Bern, Switzerland.

Bogota, Columbia (APO, Miami 34038).

Bonn, Germany (Box 310, APO, New York 09080).

Bridgetown, Barbados (Box B, FPO, Miami 34054).

Brussels, Belgium (APO, New York 09667).

Canberra, Australia (APO, San Francisco 96404–0001).

Caracas, Venezuela (Unit 4966, APO AA 34037).

Hong Kong, B.C.C. (FPO, San Francisco 96659–0002).

London, England (Box 2, FPO, New York 09509).

Madrid, Spain (PSC 61, Box 0001, APO AE 09642).

Manila, Philippines (APO, San Francisco 96528).

Mexico City, Mexico (POB 3087, Laredo, TX 78044–3087).

Montevideo, Uruguay (APO, Miami 34035).

Ottawa, Canada.

Panama City, Panama (Box E, APO, Miami 34002).

Paris, France (APO, New York 09777).

Rome, Italy (APO, New York 09794).

Tokyo, Japan (APO, San Francisco 96503).

Vienna, Austria (Unit 27937, Box 37, APO AE 09222).

[\[TOP\]](#)

JUSTICE/FBI–003

System name:

Bureau Mailing Lists.

System location:

Records may be maintained at all locations at which the Federal Bureau of Investigation

operates, including: J. Edgar Hoover Bldg., 935 Pennsylvania Ave., NW., Washington, DC 20535; FBI Academy, Quantico, VA 22135; FBI Criminal Justice Information Services (CJIS) Division, 1000 Custer Hollow Rd., Clarksburg, WV 26306; and FBI field offices, legal attachés and information technology centers as listed on the FBI's Internet website, <http://www.fbi.gov>, including any future revisions to the website.

Categories of individuals covered by the system:

All persons appearing on mailing lists maintained throughout the FBI to facilitate mailing to multiple addressees in furtherance of FBI activities. These include persons who have requested Bureau material, persons who are routinely forwarded unsolicited Bureau material and who meet established criteria (generally law enforcement or closely related interest persons who may be in a position to furnish assistance in furtherance of the FBI's mission). These do not include persons on mailing lists not encompassed within this system as described in the section titled "Categories of Records in the System."

Categories of records in the system:

Records may include name, address, business affiliation, and supplemental information to addressees and relevant to a list's purpose. These do not, however, include mailing lists which have been incorporated into some other FBI records system, such as a mailing list supporting a particular investigation maintained as an investigative record within the FBI Central Records System.

Authority for maintenance of the system:

Title 5, United States Code, section 301; title 44, United States Code, section 3101; title 28, United States Code, section 533; and title 28, Code of Federal Regulations, section 0.84.

Purpose(s):

System records are used for mailing FBI material to multiple addressees, via hard copy, or other means of distribution, in furtherance of FBI activities. For example, various fugitive alerts are furnished to local law enforcement agencies, investigations periodicals are provided to law enforcement professionals, and information on local law enforcement issues may be provided to community leaders.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The FBI may disclose relevant system records in accordance with any blanket routine use established for FBI records systems. See Blanket Routine Uses Applicable for FBI records systems. See Blanket Routine Uses Applicable to More Than One FBI Privacy Act System Records, Justice/FBI-BRU, as published today in the *Federal Register* (and any future revisions).

In addition, as a routine use specific to this system, the FBI may disclose relevant system records to the following persons or entities under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purpose for which information was collected. (Routine uses are not meant to be mutually exclusive and may overlap in some cases.)

A. To a federal, state, local, joint, tribal, foreign, international, or other public agency/organization, or to any person or entity in either the public or private sector, domestic or foreign, where such disclosure may promote, assist, or otherwise serve law enforcement interests. By way of example and not limitation, such disclosures may for instance include: Sharing names of law enforcement professionals receiving FBI periodicals with law enforcement agencies interested in reaching similar audience; sharing information of intelligence value with other law enforcement or intelligence agencies to whose lawful responsibilities the information may be germane; or sharing information pertinent to victim/witness assistance with local government entities for furtherance of such assistance.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Most information is maintained in computerized form and stored in memory, on disk storage, computer tape, or other computer media. However, some information may also be maintained in hard copy (paper) or other form.

Retrievability:

Information typically will be retrieved by an ID number assigned by computer or by name of person or organization.

Safeguards:

System records are maintained in limited access space in FBI facilities and offices. Computerized data is password protected. All FBI personnel are required to pass an extensive background investigation. The information is accessed only by authorized FBI personnel. Non-FBI personnel properly authorized to assist in the conduct of an agency function review these records.

Retention and disposal:

FBI offices revised the lists as necessary. The records are destroyed, under authority granted by the National Archives and Records Administration, when administrative needs are satisfied (Job. No. NC1-65-82-4, part E, item 13 (I)).

System manager(s) and address:

Director, FBI, 935 Pennsylvania Ave., NW, Washington, DC 20535-0001.

Notification procedure:

Same as Record Access Procedures.

Record access procedures:

A request for access to a record from the system shall be made in writing with the envelope and the letter clearly marked "Privacy Act Request". Include in the request your full name and complete address. The requester must sign the request; and, to verify it, the signature must be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. You may submit any other identifying information you wish to furnish to assist in making a proper search of the system. Requests for access to information maintained at FBI Headquarters must be addressed to the Director, Federal Bureau of Investigation, 935 Pennsylvania Ave., NW, Washington, DC 20535-0001. Requests for information maintained at FBI field offices, legal attaches, information technology centers,

or other locations must be made separately and addressed to the specific field office, le
attache, information technology center, or other location as listed on the FBI's Internet v
<http://www.fbi.gov>, including any future revisions to the website.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should al
direct their request to the appropriate FBI office, stating clearly and concisely what infor
is being contested, the reasons for contesting it, and the proposed amendment to the
information sought.

Record source categories:

The mailing list information is based on information supplied by affected
individuals/organizations, public source data, and/or information already in other FBI rec
systems.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/FBI-006

System name:

Electronic Surveillance (ELSUR) Indices.

System location:

Records may be maintained at all locations at which the Federal Bureau of Investigation
operates, including: J. Edgar Hoover FBI Bldg., 935 Pennsylvania Ave., NW., Washing
20535; FBI Academy and FBI Laboratory, Quantico, VA 22135; FBI Criminal Justice Infc
Services (CJIS) Division, 1000 Custer Hollow Rd., Clarksburg, WV 26306; FBI field offic
legal attaches, and information technology centers as listed on the FBI's Internet Web s
<http://www.fbi.gov>, including any future revisions to the Web site.

Categories of individuals covered by the system:

Individuals and entities who have been the targets of electronic surveillance coverage sought, conducted, or administered by the FBI pursuant to a court order, consensual monitoring or other authority; those who have been a party to a communication or present in a locale monitored/recorded electronically pursuant to such electronic surveillance; those who own, lease, license, hold a possessory interest in, or commonly use the property or location subjected to such electronic surveillance; and those involved in the administration of the electronic surveillance, for example, the judge issuing or denying an order for an electronic surveillance application, the prosecuting attorney, and the officials who authorized the filing of the application.

Categories of records in the system:

The ELSUR Indices are comprised of four types of records:

1. Principal records identify, by true name or best known name, all persons, entities, and facilities who have been the targets of electronic surveillance coverage sought, conducted, or administered by the FBI pursuant to a court order or other authority. These records include but are not limited to, persons, entities, and facilities named in an application filed in support of an affidavit seeking a court order to conduct or administer an electronic surveillance. Principal records may also include descriptive data associated with the name appearing on the record.
2. Proprietary-interest records identify entities and/or individuals who own, lease, license, hold a possessory interest in, or commonly use the property or location subjected to an electronic surveillance. Proprietary interest records may identify individuals involved in the administration of the electronic surveillance; for example, the judge issuing or denying an order for an electronic surveillance application, the prosecuting attorney, the officials who authorized the filing of the application. Proprietary-interest records may also include descriptive data associated with the name appearing on the record.
3. Intercept records identify, by true name or best known name, individuals who have been reasonably identified by a first name or initial and a last name as being a party to a communication monitored/recorded electronically pursuant to an electronic surveillance. Intercept records also identify entities that have been a party to a communication or present in a locale monitored/recorded electronically pursuant to an electronic surveillance. Intercept

records may include descriptive data associated with the name appearing on the record

4. Reference records identify, by partial name, such as a first name only, last name only name, nickname, or alias those individuals who have been a party to a communication captured and present in a locale monitored/recorded electronically pursuant to an electronic surveillance and may include descriptive data associated with the individual. If the individual is later identified by a more complete name, e.g., through further monitoring or normal investigation procedures, the reference record is re-entered as an intercept record.

Authority for maintenance of the system:

The ELSUR Indices were initiated in October, 1966, at the recommendation of the Department of Justice and relate to electronic surveillance sought, administered, and/or conducted by the FBI since January 1, 1960. The authority for the maintenance of these records is title 5, United States Code, section 301; title 44, United States Code, section 3101; title 18, United States Code, section 2510, et seq.; title 18, United States Code, section 3504; title 28, United States Code, section 533; title 50, United States Code 1801, et seq.; and title 28, Code of Federal Regulations, section 0.85.

Purpose(s):

These records are used by the FBI to maintain certain information regarding electronic surveillance sought, conducted or administered by the FBI in order to permit the agency to respond to judicial inquiries about possible electronic surveillance coverage of any individual entity, and to enable the Government to certify, as requested by federal, state or local law enforcement agencies, whether or not an individual, entity, facility, or place on whom a warrant or ordered authority is being sought for electronic surveillance coverage has ever been subjected to electronic surveillance coverage in the past.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The FBI may disclose relevant system records in accordance with any current and future blanket routine uses established for FBI records systems. See Blanket Routine Uses (B) Applicable to More Than One FBI Privacy Act System of Records, Justice/FBI-BRU, published on June 22, 2001 at 66 FR 33558 and amended in today's *Federal Register* (and any future revisions).

In addition, as routine uses specific to this system, the FBI may disclose relevant system records to the following persons or entities under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purpose for which the information was collected. (Routine uses are not meant to be mutually exclusive and may overlap in some cases.)

A. To the judiciary in response to inquiries about possible electronic surveillance coverage of any individual or entity.

B. To federal, state, local and tribal law enforcement officers to enable the government to certify whether or not an individual, entity, facility, or place on whom a court ordered audit is being sought for electronic surveillance coverage has ever been subjected to electronic surveillance coverage in the past.

C. To a federal, state, local, joint, tribal, foreign, international, or other public agency/organization, where such disclosure serves a law enforcement purpose, such as sharing information of intelligence value with other law enforcement or intelligence agency whose lawful responsibilities the information may be germane.

D. To any person or entity in either the public or private sector, domestic or foreign, if disclosure by the FBI to be reasonably necessary in eliciting information or cooperation from the recipient for use by the FBI in the performance of an authorized function, e.g., disclosure of personal information to a member of the public in order to elicit his/her assistance/cooperation in criminal, security, or employment background investigation.

E. To any person or entity in either the public or private sector, domestic or foreign, where there is reason to believe that a person or entity could become the target of a particular criminal activity or conspiracy, to the extent the disclosure of information is deemed by the FBI to be reasonable and relevant to the protection of life, health, or property of such target.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

The majority of the records are maintained in an automated data base. Some records are

maintained in hard-copy (paper) format or other form.

Retrievability:

Information typically will be retrieved by the name of the individual or entity. Telephone numbers and other such serial or identification numbers are retrievable numerically. Locations targeted are retrievable by street name.

Safeguards:

System records are maintained in limited access space in FBI facilities and offices. Computerized data is password protected. All FBI personnel are required to pass an external background investigation. The information is accessed only by authorized DOJ personnel. Non-DOJ personnel properly authorized to assist in the conduct of an agency function may have access to these records.

Retention and disposal:

A reference record is purged if the individual is later identified by a more complete name and converted to an intercept record. Remaining reference records are purged from the system as follows. Those relating to court ordered electronic surveillance are purged six months from the date the corresponding authorization for the surveillance expires. Reference records relating to consensual intercepts are purged one year from the last intercept date shown on the record. Until advised to the contrary by the Department of Justice, the courts, or applicable legislation, all other indices records will be maintained indefinitely and have been declared permanent by the National Archives and Records Administration (NARA) (Job No. NC1-65-82-4, Part 2(t)).

System manager(s) and address:

Director, Federal Bureau of Investigation, 935 Pennsylvania Avenue, NW., Washington, DC 20535.

Notification procedure:

Same as Record Access Procedures.

Record access procedures:

A request for notification as to whether a record about an individual exists in the system for access to a record from the system shall be made in writing with the envelope and the clearly marked "Privacy Act Request." Include in the request your full name and complete address. The requester must sign the request; and, to verify it, the signature must be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. You may submit any other identifying data you wish to furnish to assist in making a proper search of the system. Requests for access to information maintained at FBI Headquarters must be addressed to the Record/Information Dissemination Section, Federal Bureau of Investigation, 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001. Requests for information maintained at FBI field offices, information technology centers, or other locations must be made separately and addressed to the specific field information technology center, or other location as listed on the FBI's Internet Web site, <http://www.fbi.gov>, including any future revisions to the Web site.

Some information may be exempt from notification and/or access procedures as described in the section titled "Exemptions Claimed for the System." An individual who is the subject of one or more records in this system may be notified of records that are not exempt from notification and may access those records that are not exempt from disclosure. A determination on notification and access will be made at the time a request is received.

Contesting record procedures:

If you desire to contest or amend information maintained in the system, you should also include your request to the appropriate FBI office, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Some information may be exempt from contesting record procedures as described in the section titled "Exemptions Claimed for the System." An individual who is the subject of one or more records in this system may contest and pursue amendment of those records that are not exempt. A determination whether a record may be subject to amendment will be made at the time a request is received.

Record source categories:

Information in the indices is derived from electronic surveillance, public source information, other FBI record systems.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(4)(G) and (H), (e)(5) and (8), (f), (g) and (m) of the Privacy Act pursuant to 552a(j). Rules have been promulgated in accordance with the requirements of 5 U.S.C. (c) and (e), have been published in the *Federal Register*, and are codified at 28 CFR 16 and (d).

[\[TOP\]](#)

JUSTICE/FBI-007

System name:

FBI Automated Payroll System.

System location:

Federal Bureau of Investigation, J. Edgar Hoover Bldg., 10th and Pennsylvania Avenue
Washington, DC 20535.

Categories of individuals covered by the system:

(A) Current employees of the Federal Bureau of Investigation (FBI), (B) Resigned employees of the FBI are retained in the automated file for the current year for the purpose of clearing actions and providing for any retroactive actions and accounting that might be legislated.

Categories of records in the system:

System contains full record for each employee reflecting all elements relative to payroll plus accounting records and authorization records through which payrolls are issued and by which payrolls are audited. For example, this system contains the employees' Social Security Number, annual salary, time and attendance data, and job assignment.

Authority for maintenance of the system:

System is established and maintained in accordance with Federal pay requirements, and legislative enactments, Office of Personnel Management regulations, General Accounting Office rulings and decisions. Treasury Department regulation, and Office of Management and Budget regulations relative thereto, Title 5, U.S. Code, section 301 and title 44, U.S. Code, section 3101.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Biweekly issuance of payroll and related matters. Quarterly issuance of State Tax Report, Federal Insurance Contributions Act Report. Resign and End-of-Year Federal Tax Reports (W-2's), Biweekly, quarterly, fiscal and annual Budget and Accounting Reports. Appropriate information is made available to the Internal Revenue Service, Social Security Administration (to compute future entitlement to Social Security payments and Medicare/Medicaid benefits), Thrift Board (to report Thrift Savings Plan contributions so the Thrift Board can compute annuities), and state and city tax bureaus.

In addition, information may be released to the news media and the public pursuant to 5 U.S.C. 552, 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

To a Member of Congress or staff acting upon the member's behalf when the member requests the information on behalf of and at the request of the individual who is the subject of the record; and,

To the National Archives and Records Administration and the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or

official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored electronically on magnetic tapes and diskettes and is accessible only by use in a computer environment.

Retrievability:

Information is retrieved by Social Security Number. (The authority to solicit an employee's Social Security Number is based on title 26, Code of Federal Regulations, section 31.601(b)-2(b).)

Safeguards:

Information contained in the system is relative to the individual employee's payroll status and is considered confidential to that employee and to official business conducted for that employee's pay and accounting purposes. It is safeguarded and protected in accordance with the Federal Computer Center's regulations that permit access and use by only authorized personnel.

Retention and disposal:

Master payroll and accounting records are stored electronically and retained for a period of three years. Federal tax files are retained for four years. Auxiliary files pertinent to main functions are retained for periods varying from three pay periods to three years, depending on the support files needed for any retroactive or audit purposes. (GRS 2; GSA Reg. 3; GSA B-47, "Archives and Records"; and Job No. NC1-65-82-4, part E. 13c. (1))

System manager(s) and address:

Director, Federal Bureau of Investigation, Ninth and Pennsylvania Avenue, NW, Washington, DC 20535.

Notification procedure:

Same as the above.

Record access procedures:

A request of access to information may be made by an employee through his supervisor or a former employee by writing to the Federal Bureau of Investigation, 9th and Pennsylvania Avenue, NW, Washington, DC 20535, Attention Payroll Office.

Contesting record procedures:

Contest of any information should be set out in detail and a check of all supportive records should be made to determine the factual data in existence, which is predetermined by source documents and accounting procedures governing pay matters.

Record source categories:

Source of information is derived from personnel actions, employee authorizations, and other records which are issued and recorded in accordance with regulations governing Federal personnel.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/FBI-008

System name:

Bureau Personnel Management System (BPMS).

System location:

Federal Bureau of Investigation, J. Edgar Hoover Building, 10th and Pennsylvania Avenue NW, Washington DC 20535.

Categories of individuals covered by the system:

Federal Bureau of Investigation, employees and former employees.

Categories of records in the system:

The system contains personnel information which includes information set forth on (1) Standard Form 50—Notification of Personnel Action, (2) SF 176—T—Federal Employee Civil Life Insurance Plan, (3) FBI form 12-60 in lieu of SF 1126—Notification of Pay Change, 2801 and CSC 1084—Application for and additional information in support of retirement respectively, (5) SF 2809—Federal Employment Health Benefit Plan and (6) various intra-agency forms and memoranda.

Authority for maintenance of the system:

The system is established and maintained pursuant to regulations set forth in the Federal Personnel Manual, title 5, U.S. Code, section 301 and title 44, U.S. Code, section 3101.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The BPMS is used (1) to prepare the Notification of Personnel Action, copies of which are furnished to the Office of Personnel Management, (2) to prepare Standard Form 52B—Request for Personnel Action, (3) to generate lists of employees which are used internally by authorized personnel for recordkeeping, planning, and decision making purposes and (4) as a source for the dissemination of information (A) to federal, state and local agencies and to private organizations pursuant to service record inquiries and (B) pursuant to credit inquiries. In response to proper credit inquiries from credit bureaus and financial institutions the FBI will verify employment and furnish salary and length of service.

In addition, information may be released to the news media and the public pursuant to 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy; Member of Congress staff acting upon the member's behalf when the member or staff requests the information on behalf of and at the request of the individual who is the subject of the record; and, to the National Archives and Records Administration and the General Services Administration

records management inspections conducted under the authority of 44 U.S.C. 2904 and

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in BPMS is stored by disc and magnetic tape.

Retrievability:

Information is retrieved (1) on-line through intelligent workstations and terminals by key name or Social Security Number of the employee and (2) off-line through data base retrieval.

(It is noted the authority to solicit an employee's Social Security Number is based on title 5, Code of Federal Regulations, section 31.6011(b)-2(b).)

Safeguards:

Areas housing the system and access terminals are located in secure buildings available only to authorized FBI personnel and escorted maintenance and repair personnel only. Access terminals are operational only during normal daytime working hours at which time they are constantly attended. Access through terminals is protected by sign-on and passwords.

Retention and disposal:

Electronically stored records for employees and former employees are maintained indefinitely in a vault under the control of a vault supervisor. Pursuant to regulations set forth in the Federal Personnel Manual a copy of the Notification of Personnel Action is made a part of the employee's personnel file.

employees' personnel file.

The automated records are disposable when administrative needs have expired. (Job N NC1-65-82-4, part E. 13c.(1)).

System manager(s) and address:

Director, Federal Bureau of Investigation, John Edgar Hoover Building, 10th Street and Pennsylvania Avenue, NW, Washington, DC 20535.

Notification procedure:

Same as the above.

Record access procedures:

A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." Include in the request the name and return address of the requestor. Access requests will be directed to the Director, Federal Bureau of Investigation.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the Director, FBI stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in this system are present and former FBI employees and employee personnel files.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/FBI-009

System name:

Fingerprint Identification Records System (FIRS).

System location:

Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division, 1 Custer Hollow Road, Clarksburg, WV 26306.

Categories of individuals covered by the system:

- A. Individuals fingerprinted as a result of arrest or incarceration.
- B. Persons fingerprinted as a result of federal employment application or military service; in addition, there are a limited number of persons fingerprinted for alien registration and naturalization purposes and a limited number of individuals desiring to have their fingerprints placed on record with the FBI for personal identification purposes.

Categories of records in the system:

- A. Criminal fingerprints and/or related criminal justice information submitted by authorized agencies having criminal justice responsibilities.
- B. Civil fingerprints submitted by federal agencies and civil fingerprints submitted by persons desiring to have their fingerprints placed on record for personal identification purposes.
- C. Identification records sometimes referred to as "rap sheets," which are compilations of criminal history record information pertaining to individuals who have criminal fingerprints maintained in the system.
- D. A name index pertaining to all individuals whose fingerprints are maintained in the system.

Authority for maintenance of the system:

The system is established and maintained under authority granted by 28 U.S.C. 534, Pub. L. 92-544 (86 Stat. 1115), and codified in 28 CFR 0.85 (b) and (j) and part 20. Additional uses are also listed below under Routine Uses.

Purpose(s):

The purpose for maintaining the Fingerprint Identification Records System is to perform identification and criminal history record information functions and maintain resultant records for local, state, tribal, federal, foreign, and international criminal justice agencies, as well as noncriminal justice agencies and other entities where authorized by federal statute, state statute pursuant to Pub. L. 92-544, Presidential executive order or regulation of the Attorney General of the United States. In addition, identification assistance is provided in disaster relief and for other humanitarian purposes.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Identification and criminal history record information within this system of records may be disclosed as follows:

1. To a local, state, tribal, or federal law enforcement agency, or agency/organization directly engaged in criminal justice activity (including the police, prosecution, penal, probation/prison, and the judiciary), and/or to an authorized foreign or international agency/organization, such disclosure may assist the recipient in the performance of a law enforcement function and/or for the purposes of eliciting information that may assist the FBI in performing a law enforcement function; or to a local, state, tribal, federal, foreign, or international agency/organization for a compatible civil law enforcement function; or where such disclosure may promote, assist, or otherwise serve the mutual law enforcement efforts of the law enforcement community.
2. To a federal, state, tribal, or local criminal or noncriminal justice agency/organization; or other entities where specifically authorized by federal statute, state statute pursuant to Pub. L. 92-544, Presidential executive order, or regulation of the Attorney General of the United States for use in making decisions affecting employment, security, contracting, licensing, revocation, or other suitability determinations. Examples of these disclosures may include the release of information as follows:

- a. To the Department of Defense, Department of State, Office of Personnel Management, Central Intelligence Agency, when requested for the purpose of determining the eligibility of a person for access to classified information or assignment to or retention in sensitive national security duties. 5 U.S.C. 9101 (1990);
- b. To federal agencies for use in investigating the background of present and prospective federal employees and contractors (Executive Order 10450), including those providing child-care services to children under age 18 at each federal agency and at any facility owned or under contract by the federal government. 42 U.S.C. 13041 (1991);
- c. To state and local government officials for purposes of investigating the background of applicants for noncriminal justice employment or licensing purposes if such investigation is authorized by a state statute that has been approved by the Attorney General of the United States. (The Attorney General has delegated to the FBI the responsibility for approving state statutes.) Examples of applicants about whom FIRS information may be disclosed include: Providers of services/ care for children, the elderly, or disabled persons; teachers/school bus drivers; adoptive/foster parents; security guards/private detectives; bar applicants; doctors; and explosive dealers/purchasers. Pub. L. 92-544, 86 Stat. 1111 (1972);
- d. To officials of state racing commissions for use in investigating the background of an applicant for a state license to participate in parimutuel wagering. Officials of state racing commissions in states with a state statute that has been approved under Pub. L. 92-544 submit fingerprints of the applicant to the FBI through the Association of State Racing Commissioners International, Inc. Results of a criminal record check are returned to each racing commission designated on the fingerprint card. Pub. L. 100-413, 102 Stat. 1101; (1988);
- e. To officials of Indian tribal governments for use in investigating the background of an applicant for employment by such tribes in a position involving regular contact with, or care of, Indian children. Officials may submit fingerprints to the FBI through the Bureau of Indian Affairs and the results of the criminal record check are returned to the Bureau of Indian Affairs for transmittal to the appropriate tribal government. Pub. L. 101-630; 25 U.S.C. 3205; 25 U.S.C. 3207;
- f. To a designated point of contact at a criminal justice agency for the conduct of background checks under the National Instant Criminal Background Check System (NICS).

g. To criminal justice officials for the conduct of firearms related background checks which are required to issue firearms or explosive related licenses or permits according to a state or local ordinance. Fingerprints submitted for this noncriminal justice purpose, as well as criminal justice related permits, are processed pursuant to Pub. L. 92-544 as set out under 2.C. above. Pub. L. 103-159; 18 U.S.C. 922;

h. To officials of federally chartered or insured banking institutions for use in investigating the background of applicants for employment or to otherwise promote or maintain the security of those institutions. Pub. L. 92-544; 86 Stat. 1115;

i. To officials of the Securities and Exchange Commission (SEC) and to self-regulatory organizations (SRO) designated by the SEC for use in investigating all partners, directors, officers, and employees involved in the transfers/handling of securities at every member of a national securities exchange, broker, dealer, registered transfer agent, and registered clearing agency. (The SROs are: American Stock Exchange, Boston Stock Exchange, Chicago Board of Options Exchange, Midwest Stock Exchange, New York Stock Exchange, Pacific Stock Exchange, Philadelphia Stock Exchange, and the National Association of Securities Dealers). 15 U.S.C. 78q(f)(2) (1990);

j. To officials of the Commodity Futures Trading Commission (CFTC) and the National Futures Association for use in investigating the background of applicants for registration with the CFTC as commodity dealers/members of futures associations. Such applicants include futures commission merchants, introducing brokers, commodity trading advisors, commodity pool operators, floor brokers, and associated persons. 7 U.S.C. 12a (1992); 7 U.S.C. 21(b)(4) (1992);

k. To officials of the Nuclear Regulatory Commission (NRC) for use in investigating the background of each individual who is permitted unescorted access to a nuclear utilization facility (nuclear power plant) and/or who is permitted access to information relating to the safeguarding of such facilities. 42 U.S.C. 2169 (1992).

3. To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies.

4. To private contractors pursuant to a specific agreement with a criminal justice agency or noncriminal justice governmental agency performing criminal justice dispatching functions or data processing/information services for criminal justice agencies to provide services for

administration of criminal justice pursuant to that agreement. The agreement must include a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

5. To the news media and general public where there exists a relevant and legitimate public interest (unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy) and where disclosure will serve a relevant and legitimate law enforcement function, e.g., to assist in locating federal fugitives, and to provide notification of arrests. This would include disclosure of information in accordance with 23 CFR 20.33 (a)(4) and (c), and 50.2. In addition, where disclosure is relevant and necessary to protect the general public or any member of the public from imminent threat to life, bodily injury, or property, such information may be disclosed.

6. To a Member of Congress or staff acting on the Member's behalf when the Member requests the information on behalf of and at the request of the individual who is the subject of the record.

7. To the National Archives and Records Administration and the General Services Administration for records management inspections and such other purposes conducted under the authority of 44 U.S.C. 2904 and 2906, to the extent that such legislation requires or authorizes the disclosure.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

- A. The criminal fingerprints and related criminal justice information are stored in both automated and manual formats. The manual records are in file cabinets in their original on microfilm.
- B. The civil fingerprints are stored in an entirely manual format.
- C. The identification records or "rap sheets" are mostly automated but a significant portion of older records are manual.
- D. The criminal name index is either automated or on microfilm while the civil name index is entirely manual.

Retrievability:

- A. Information in the system is retrievable by technical fingerprint classification and position. Identification is effected only by comparison of unique identifying characteristics appearing on fingerprint impressions submitted for search against the fingerprints maintained within the system.
- B. An auxiliary means of retrieval is through name indices which contain names of the individuals, their birth data, other physical descriptors, and the individuals' technical fingerprint classification and FBI numbers, if such have been assigned.

Safeguards:

Information in the system is unclassified. Disclosure of information from the system is made only to authorized recipients upon authentication and verification of the right to access the system by such persons and agencies. The physical security and maintenance of information within the system is provided by FBI rules, regulations and procedures.

Retention and disposal:

- A. The Archivist of the United States has approved the destruction of records maintained in a criminal file when the records indicate individuals have reached 99 years of age, and the

destruction of records maintained in the civil file when the records indicate individuals have reached 99 years of age. (Job. No. N1-65-95-03)

B. Fingerprints and related arrest data in the system are destroyed seven years following notification of the death of an individual whose record is maintained in the system (Job. No. N1-65-95-03)

C. The Archivist has determined that automated FBI criminal identification records (rap sheets) are to be permanently retained. Thus, at the time when paper identification records would have been eligible for destruction, automated FBI criminal identification records are transferred from magnetic tape to NARA.

D. Fingerprints submitted by state and local criminal justice agencies are removed from the system and destroyed upon the request of the submitting agencies. The destruction of fingerprints under this procedure results in the deletion from the system of all arrest information related to those fingerprints.

E. Fingerprints and related arrest data are removed from the Fingerprint Identification Records System upon receipt of federal court orders for expunction when accompanied by necessary identifying information. Recognizing lack of jurisdiction of local and state courts over an agency of the federal government, the Fingerprint Identification Records System, as a matter of course, destroys fingerprints and related arrest data submitted by local and state criminal justice agencies upon receipt of orders of expunction directed to such agencies by local and state courts when accompanied by necessary identifying information.

System manager(s) and address:

Director, Federal Bureau of Investigation, J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW, Washington, DC 20535-0001.

Notification procedure:

This system has been exempted from subsections (d) and (e)(4)(G) pursuant to subsections (j)(2), (k)(2), and (k)(5) of the Privacy Act.

Record access procedures:

This system of records has been exempted from subsections (d) and (e)(4)(H) pursuant subsections (j)(2), (k)(2), and (k)(5) of the Privacy Act. However, procedures are set forth in CFR 16.30–34 and 20.24 for an individual to obtain a copy of his identification record maintained in the Fingerprint Identification Records System to review or to obtain a character correction, or updating of the record.

Contesting record procedures:

Same as above.

Record source categories:

Federal, state, local, tribal, foreign, and international agencies. See Categories of Individuals Covered by the System.

Exemptions claimed for the system:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d); (e)(3), (4)(G) and (H), (5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). In addition, the Attorney General has exempted this system from (c)(3), (d), (e)(1), and (e)(4)(H), pursuant to (k)(2) and (k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/FBI-010

System name:

Employee Travel Vouchers and Individual Earning Records.

System location:

Federal Bureau of Investigation, J. Edgar Hoover Bldg., 10th and Pennsylvania Avenue, NW, Washington, DC 20535. Records pending audit are located at Federal Records Centers.

Categories of individuals covered by the system:

Former and current employees of the FBI.

Categories of records in the system:

Payroll, travel and retirement records of current and former employees of the FBI.

Authority for maintenance of the system:

The head of each executive agency, or his delegate, is responsible for establishing and maintaining an adequate payroll system, covering pay, leave and allowances, as a part system of accounting and internal control of the Budget and Accounting Procedures Act of 1950, as amended, 31 U.S.C. 66, 66a, and 200(a).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records are used by Departmental personnel to prepare and document payment to employees of the FBI and to carry out financial matters related to the payroll or accounting functions.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) and GSA in connection with management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Manual on paper files.

Retrievability:

The records can be retrieved by name; and either social security account number or em identification number.

Safeguards:

Accessed by Bureau employees at FBI Headquarters and by Field Office employees at Records Centers. Transmittal document contains Bureau statement concerning security who may access or view records. Records are maintained in rooms under the control of employees during working hours and maintained in locked file cabinets in locked rooms other times. Security guards further restrict access to the building to authorized personr only.

Retention and disposal:

Employee Travel Vouchers are destroyed 6 years, 3 months, after the period covered by account (GRS No. 6, Item 1A2). Individual Earnings Records are destroyed 56 years aft of last entry (GRS No. 2, Item 1).

System manager(s) and address:

Director, Federal Bureau of Investigation, 9th and Pennsylvania Avenue, NW, Washingt 20535.

Notification procedure:

Written inquiries, including name, date of birth, and social security number, to determin whether this system contains records about an individual may be addressed to Director, Federal Bureau of Investigation, 9th and Pennsylvania Avenue, NW, Washington, DC 2

Record access procedures:

Contesting record procedures:

Written inquiries, including name, date of birth and social security number, requesting a correction or contesting the accuracy of records may be addressed to: Director, Federal Bureau of Investigation, 9th and Pennsylvania Avenue, NW, Washington, DC 20535.

Record source categories:

Travel vouchers turned in by individual employees for official business. Pay records—time and attendance records, pay determined by the agency.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/FBI-011

System name:

Employee Health Records.

System location:

Federal Bureau of Investigation, Administrative Services Division, Health Service, J. Edgar Hoover Bldg., 10th and Pennsylvania Avenue, NW, Washington, DC 20535 and the following field offices: New York, Newark, Philadelphia, Chicago, Los Angeles, San Francisco, San Diego, Quantico, Virginia. Addresses for field offices can be found in the appendix of the System notice Justice/FBI 002.

Categories of individuals covered by the system:

Current and former employees of the FBI.

Categories of records in the system:

Records of visits to health facilities relating to sickness, injuries or accidents.

Authority for maintenance of the system:

The head of each agency is responsible, under 5 U.S.C. 7902, for keeping a record of illness and accidents to its employees and for reducing accidents and health risks. These records are maintained under the general authority of 5 U.S.C. 301 so that the FBI can be kept aware of the health related matters of its employees and more expeditiously identify them.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records are maintained by the FBI to identify matters relating to the health of its present and former employees. Information is available to employees of the FBI whose job function relates to identifying and resolving health matters of former and current personnel of the FBI.

In addition, information may be released to the National Archives and Records Administration and the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining and disposing of records in the system:

Storage:

Previous procedure of creation and maintenance of 3 0A 5 index cards to record individual health service visits has been phased out and a clinical folder is created to maintain an employee health record and SF 510, "Nursing Notes" . The information is maintained in the

in a file folder.

Retrievability:

By name.

Safeguards:

These records are maintained by FBI personnel during working hours and in locked file cabinets during non-working hours. Security guards further restrict access to the building to authorized personnel.

Retention and disposal:

Remaining index cards will be destroyed 6 years after date of last entry (GRS #1, Item 1 folder containing the health record and nursing notes will be transferred to the employee medical folder, an appendage of the Office Personnel Folder, when Health Unit is notified of resignations or retirements.

System manager(s) and address:

Director, Federal Bureau of Investigation, 9th and Pennsylvania Avenue, NW, Washington, DC 20535.

Notification procedure:

Written inquiries, including name, address and social security number, to determine whether this system of records contains records about an individual may be addressed to Director, Federal Bureau of Investigation, 9th and Pennsylvania Avenue, NW, Washington, DC 20535 and/or individually to the field offices which maintain similar records.

Record access procedures:

Contesting record procedures:

Written inquiries, including name, date of birth and social security number, requesting access to or contesting the accuracy of records may be addressed to: Director, Federal Bureau of Investigation, 9th and Pennsylvania Avenue, NW, Washington, DC 20535.

Investigation, 9th and Pennsylvania Avenue, NW, Washington, DC 20535, and the above mentioned field offices at addresses referred to in system notice Justice/FBI 002.

Record source categories:

Employees of the Federal Bureau of Investigation originate their own records. Nursing records appear on SF 510.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/FBI-012

System name:

Time Utilization Record/Keeping (TURK) System.

System location:

Administrative Services Division, Federal Bureau of Investigation, J. Edgar Hoover Building, 10th and Pennsylvania Avenue, NW, Washington, DC 20535.

Categories of individuals covered by the system:

Special Agents, Accounting Technicians, Investigative Assistants, and Laboratory Technicians.

Categories of records in the system:

System contains by-weekly time utilization data of Special Agents, Accounting Technicians, Investigative Assistants and Laboratory Technicians.

Authority for maintenance of the system:

This system of records is maintained under the authority of 31 U.S.C. 66a which requires

head of the Department, or his delegate, to establish a system of accounting and intern control designed to provide full disclosure of the financial results of the FBI's activities; adequate financial information needed for the FBI's management purposes and effective control over and accountability for all funds, property and other assets for which the FBI is responsible.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

For the purpose of producing cost accounting reports reflective of personnel utilization, may be made available to the General Accounting Office, the Office of Management and Budget and the Treasury Department.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Information maintained in the system is stored electronically on magnetic tapes and disk use in a computer environment.

Retrievability:

Information is retrieved by name and/or social security number and summarized by Computer Center.

Safeguards:

Information is safeguarded and protected in accordance with the FBI's Computer Center

regulations that permit access and use by authorized personnel only.

Retention and disposal:

Biweekly magnetic tapes and discs are retained for a period of 3 years. Hard copy records are retained in accordance with instructions contained in GRS No. 8, Items 7 and 8, and GSA Bulletin FPMR-47, "Archives and Records". Hard copy records are destroyed; magnetic records are erased and reused. (Job No. NCI-65-82-4, part E. 13c. (1)).

System manager(s) and address:

Director, Federal Bureau of Investigation, 9th and Pennsylvania Avenue, NW, Washington, DC 20535.

Notification procedure:

Same as above.

Record access procedures:

Same as above.

Contesting record procedures:

Written requests for access to information may be made by an employee through his supervisor or by former employees by writing to: Federal Bureau of Investigation, 9th and Pennsylvania Avenue, NW, Washington, DC 20535 (Attn: Administrative Services Division). Contesting of any information should be set out in written detail and forwarded to the above address. A check of all supportive records will be made to determine the factual data in existence.

Record source categories:

Source of information is derived from daily time utilization recording made by the employee.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/FBI-013

System name:

Security Access Control System (SACS).

System location:

Records may be located at all locations at which the Federal Bureau of Investigation (FBI) operates, including: J. Edgar Hoover FBI Building, 935 Pennsylvania Ave., NW., Washington, DC 20535; FBI Academy and FBI Laboratory, Quantico, VA 22135; FBI Criminal Justice Information Services (CJIS) Division, 1000 Custer Hollow Rd., Clarksburg, WV 26306; FBI field offices, legal attaches, and information technology centers as listed on the FBI's Internet site, <http://www.fbi.gov>, including any future revisions to the Web site.

Categories of individuals covered by the system:

All individuals who have applied for, sought, been considered for, attempted and/or obtained access to the J. Edgar Hoover FBI Building, FBI field offices, CJIS West Virginia Complex, FBI Academy, FBI Laboratory, legal attaches, information technology centers or other locations where the FBI operates, or to FBI vehicles, property or equipment, including: current and former FBI employees, contractors, vendors, grantees, experts, consultants, task force personnel, volunteers, detailees, visitors, and other non-FBI employees. May also include persons identified as employers, sponsors, references, or contacts for the above individuals.

Categories of records in the system:

Records may include: names; social security numbers; dates of birth; physical descriptions; badge numbers; information on employer, sponsor, contacts, and/or references; home and business addresses and phone numbers; dates and times of entry, exit, and/or passage through control points; fingerprints, photographs, videos, electronic images, signatures, other biometric identifiers; vehicle identification data; purpose of visit and person visited; and other related information.

Authority for maintenance of the system:

Executive Order 12958, as amended 13292, Title 5 U.S.C. 552a(e)(10); title 44 U.S.C. ch 21 and 33. These statutes, as well as the Executive Orders, are directed toward security of United States Government records maintained by federal agencies. Title 40 U.S.C. chap 318a; and Title 41 CFR 102–81.10 and 81.15. This statute and the federal regulations are directed toward security of United States Government buildings and the people therein.

Purpose(s):

System records are necessary to maintain the security of the personnel and locations at which the FBI operates, and of FBI records, vehicles, property and equipment, and are used to determine eligibility and/or the status of individuals who have applied for, sought, been considered for, attempted and/or obtained such access. System records are also used to maintain control of badges issued for access to locations where the FBI operates and to Bureau vehicles, property or equipment.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The FBI may disclose relevant system records in accordance with any current or future routine uses established for FBI records systems. See Blanket Routine Uses (BRU) App to More Than One FBI Privacy Act System of Records, Justice/FBI–BRU, published on 12/22, 2001 at 66 FR 33558 and amended in today's *Federal Register* (and any future revisions).

In addition, as routine uses specific to this system, the FBI may disclose relevant system records to the following persons or entities under the circumstances or for the purposes described below, to the extent such disclosures are compatible with the purpose for which the information was collected. (Routine uses are not meant to be mutually exclusive and may overlap in some cases.)

A. To a federal, state, local, joint, tribal, foreign, international, or other public agency/organization, where such disclosure serves a law enforcement purpose, such as sharing information of intelligence value with other law enforcement or intelligence agencies whose lawful responsibilities the information may be germane.

B. To any person or entity in either the public or private sector, domestic or foreign, if de

by the FBI to be reasonably necessary in eliciting information or cooperation from the re for use by the FBI in furthering the purposes of the system, e.g., disclosure of personal identifying information to an associate or employer of a person to confirm the person's ik suitability, and reason for access to an FBI facility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Most information is maintained in computerized form and stored in memory, on disk stor computer tape, or other computer media. However, some information may also be maini in hard copy (paper) or other form.

Retrievability:

Information is typically retrieved by name of the individual, other personal identifiers, or access badge number.

Safeguards:

System records are maintained in limited access space in FBI controlled facilities and of Computerized data is password protected. All FBI personnel are required to pass an ex background investigation. The information is accessed only by authorized DOJ personn non-DOJ personnel properly authorized to assist in the conduct of an agency function r to these records.

Retention and disposal:

System records in all formats are maintained and disposed of in accordance with appro authority of the National Archives and Records Administration.

System manager(s) and address:

Director, FBI, 935 Pennsylvania Ave., NW., Washington, DC 20535-0001.

NOTIFICATION PROCEDURES:

Same as Record Access Procedures.

Record access procedures:

A request for access to a record from the system shall be made in writing with the envelope and the letter clearly marked "Privacy Act Request" . Include in the request your full name and complete address. The requester must sign the request; and, to verify it, the signature must be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. You may submit any other identifying information you wish to furnish to assist in making a proper search of the system. Requests for access to information maintained at FBI Headquarters must be addressed to the Record/Information Dissemination Section, Federal Bureau of Investigation, 935 Pennsylvania Ave., NW., Washington, DC 20535-0001. Requests for information maintained at other FBI locations must be made separately and addressed to the specific location as listed on the FBI's Internet site, <http://www.fbi.gov>, including any future revisions to the Web site.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should always direct their request to the appropriate FBI location, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

See Categories of Individuals Covered by The System.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[\[TOP\]](#)

JUSTICE/FBI-014

System name:

FBI Alcoholism Program.

System location:

FBI Headquarters, Administrative Services Division, 10th and Pennsylvania Avenue NW Washington, DC 20535; and FBI Field Divisions.

Categories of individuals covered by the system:

This system contains information on current and former FBI employees who have been counseled or otherwise treated regarding alcohol abuse or referred to the Alcoholism Program Coordinator or Counselor.

Categories of records in the system:

This system contains correspondence and records regarding employees and/or their families who have been referred to the Alcoholism Program Coordinator or Counselor, the results of any counseling which may have occurred, recommended treatment and results of treatment in addition to interview appraisals and other notes or records of discussions held with employees relative to this program.

Authority for maintenance of the system:

The maintenance of this system is authorized by Pub. L. 91-616 and Pub. L. 92-255, as amended by Pub. L. 93-282, Section 122, and the implementing regulations, 42 CFR Part 2.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

All disclosures of information pertaining to an individual are made in compliance with Pub. L. 91-616, Section 333, and the Confidentiality of Alcoholism and Drug Abuse Patient Records Regulations, 42 CFR 2.2, as amended, for the sole purpose of administering the program.

These records are used to document the nature of an individual's alcohol abuse problem, progress made, and to record an individual's participation in and the results of community and private sector treatment or rehabilitation programs.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Records are maintained in file folders.

Retrievability:

Records are retrieved by employee's name.

Safeguards:

Files are maintained in locked file cabinets, or safes under the immediate control of the Alcoholism Program Coordinator or other authorized individuals. Access is strictly limited to the Coordinator and other authorized personnel.

Retention and disposal:

Files are destroyed 3 years after case is closed. (GRS No. 1, Item 27 b.; Job No. NC1-65-82-4, Part B. 67d.)

System manager(s) and address:

Director, FBI J. Edgar Hoover Building, 10th and Pennsylvania Avenue NW., Washington, DC 20535.

Notification procedure:

Inquiry concerning this system should be in writing and made to the system manager listed above.

Record access procedures:

Requests made by employees should be made in writing to the Director, FBI, Washington, DC 20535. Requests must contain employee's full name, date and place of birth, and current assignment and/or home address where records are to be sent. If the individual making request is a former employee, he/she must submit a duly notarized signature in order to establish identity. In addition, the requester must specify the location of the system of records sought, i.e., those maintained at FBI headquarters or those maintained in a particular field division.

Contesting record procedures:

Requests for correction/amendment of records in this system should be made in writing to the Director, FBI, Washington, DC 20535, specifying the information to be amended, and the reasons and justifications for requesting such amendment.

Record source categories:

See categories of individuals.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/FBI-015

System name:

National Center for the Analysis of Violent Crime (NCAVC).

System location:

Federal Bureau of Investigation, Training Division, FBI Academy, Behavioral Science Unit
Quantico, Virginia 22135.

Categories of individuals covered by the system:

- A. Individuals who relate in any manner to official FBI investigations into violent crimes including, but not limited to, subjects, suspects, victims, witnesses, close relatives, medical personnel, and associates who are relevant to an investigation.
- B. Individuals who are the subject of unsolicited information or who offer unsolicited information, and law enforcement personnel who request assistance and/or make inquiries concerning records.
- C. Individuals who are the subject of violent crime research studies including, but not limited to, criminal personality profiles, scholarly journals, and news media references.

Categories of records in the system'

The National Center for the Analysis of Violent Crime will maintain in both manual and automated formats case investigation reports on all forms of solved and unsolved violent crimes. These violent crimes include, but are not limited to, acts or attempted acts of murder, kidnapping, incendiary arson or bombing, rape, physical torture, sexual trauma, or evidence of violent forms of death. Less than ten percent of the records which are analyzed may not be directly related to violent activities.

- A. Violent Criminal Apprehension Program (VICAP) case reports submitted to the FBI by any constituted Federal, State, county, municipal, or foreign law enforcement agency in any criminal matter. VICAP reports include, but are not limited to, crime scene descriptions, and offender descriptive data, laboratory reports, criminal history records, court records, news media references, crime scene photographs, and statements.
- B. Violent crime case reports submitted by FBI headquarters or field offices, and case reports submitted to the FBI by a duly constituted Federal, State, county, municipal, or foreign law enforcement agency in any violent criminal matter.
- C. Violent crime research studies, scholarly journal articles, textbooks, training materials

news media references of interest to NCAVC personnel.

D. An index of all detected trends, patterns, profiles and methods of operation of known unknown violent criminals whose records are maintained in the system.

E. An index of the names, addresses, and contact telephone numbers of professional individuals and organizations who are in a position to furnish assistance to the FBI's NC operation.

F. An index of public record sources for historical, statistical and demographic data collected by the U.S. Bureau of the Census.

G. An alphabetical name index pertaining to all individuals whose records are maintained in the system.

Authority for maintenance of the system:

44 U.S.C. 3101; 41 CFR subpart 101-11.2 and 28 U.S.C. 534.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Currently, the NCAVC is administered by the FBI through its Training Division, located at the FBI Academy, Quantico, Virginia. Its primary mission is to consolidate research, training and operational support activities for the express purposes of providing expertise to any legitimate law enforcement agency confronted with unusual, bizarre, and/or particularly vicious or repetitive violent crimes.

Records described above are maintained in this system to permit the FBI to function efficiently as an authorized, responsive component of the Department of Justice. Therefore, the information in this system is disclosed to officials and employees of the Department of Justice and/or all components thereof, who need the information to perform their official duties.

Information in this system may be disclosed as a routine use to any Federal, State, local or foreign government agency directly engaged in the criminal justice process where access is directly related to a law enforcement function of the recipient agency in connection with tracking identification, and apprehension of persons believed to be engaged in repeated

exceptionally violent acts of criminal behavior.

Information in this system may be disclosed as a routine use in a proceeding before a adjudicative body, e.g., the Equal Employment Opportunity Commission and the Merit Systems Protection Board, before which the FBI is authorized to appear, when (a) the FBI is an employee thereof in his or her official capacity, or (b) any employee in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (c) the United States, where the FBI determines it is likely to be affected by the litigation, is a party to the litigation or has an interest in litigation and such records are determined by the FBI to be relevant to the litigation.

Information in this system may be disclosed as a routine use to an organization or individual in the public or private sector pursuant to an appropriate legal proceeding or, if deemed necessary, to elicit information or cooperation from the recipient for use by the FBI in the performance of an authorized activity. An example could be where the activities of an individual are disclosed to a member of the public to elicit his/her assistance in FBI apprehension and detection efforts.

Information in this system may be disclosed as a routine use to an organization or individual in the public or private sector where there is reason to believe the recipient is or could become the target of a particular criminal activity or conspiracy and to the extent the information is relevant to the protection of life or property.

Relevant information may be disclosed from this system to the news media and general public where there exists a legitimate public interest. Examples would include: To obtain public media assistance in the tracking, identifying, and apprehending of persons believed to be engaged in repeated acts of violent criminal behavior; to notify the public and/or media of arrests; to protect the public from imminent threat to life or property where necessary; and to disseminate information to the public and/or media to obtain cooperation with violent crime research, evaluation, and statistical programs.

Information in this system may be disclosed as is necessary to appropriately respond to congressional inquiries on behalf of constituents.

A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906 to the extent that legislation governing the record

permits.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information in the system is stored manually in locked file cabinets, either in its natural form or on microfilm, at the NCAVC in Quantico, Virginia. The active main files are maintained in hard copy form and some inactive records are maintained on microfilm.

In addition, some of the information is stored in computerized data storage devices at the NCAVC and FBI Computer Center in Washington, DC. Investigative information which is maintained in computerized form may be stored in memory on disk storage on computer or on computer printed listings.

Retrievability:

On-line computer access to NCAVC files is achieved by using the following search descriptions:

A. A data base which contains the names of individuals, their birth dates, physical descriptions, and other identification numbers such as FBI numbers, if such have been assigned.

B. Summary variables contained on VICAP reports submitted to the NCAVC as previously described.

C. Key words citations to violent crime research studies, scholarly journal articles, textbooks, training materials, and media references.

Safeguards:

Records are maintained in restricted areas and accessed only by FBI employees. All FBI employees receive a complete pre-employment background investigation. All employees are cautioned about divulging confidential information or any information contained in FBI files. Failure to abide by this provision violates Department of Justice regulations and may violate certain statutes providing maximum severe penalties of a ten thousand dollar fine or 10 years imprisonment or both. Employees who resign or retire are also cautioned about divulging information acquired in the job.

Registered mail is used to transmit routine hard copy records between field offices. Highly classified records are hand carried by Special Agents or personnel of the Armed Forces Courier Service. Highly classified or sensitive privacy information, which is electronically transmitted between field offices and to and from FBI Headquarters, is transmitted in encrypted form to prevent interception and interpretation.

Information transmitted in teletype form between the NCAVC in Quantico, Virginia and the FBI Computer Center in Washington, DC, is encrypted prior to transmission at both places to ensure confidentiality and security of the data.

FBI field offices involved in certain complicated, investigative matters may be provided with on-line access to the computerized information which is maintained for them on disc storage at the FBI Computer Center in Washington, DC. This computerized data is also transmitted in encrypted form.

Retention and disposal:

Records are proposed for destruction after 50 years or upon termination of the program whichever is earlier. The disposition schedule is pending with NARA as Job No. N1-65-

System manager(s) and address:

Director, Federal Bureau of Investigation, 10th and Pennsylvania Avenue NW, Washington, DC 20535.

Notification procedure:

Address inquiries to the System Manager.

Record access procedures:

Requests for access to records in this system shall be made in writing with the envelope the letter clearly marked "Privacy Access Request." The request must provide the full name, complete address, date of birth, place of birth, and notarized signature of the individual the subject of the record requested. The request should also include the general subject matter of the document or its file number—along with any other known information which assist in making a search of the records. The request must also provide a return address transmitting the information. Access requests should be addressed to the Director, Federal Bureau of Investigation, Washington, DC 20535.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should all direct their request to the Director, Federal Bureau of Investigation, Washington, DC 20535. The request should state clearly and concisely (1) the reasons for contesting the information and (2) the proposed amendment to the information.

Record source categories:

The FBI, by the very nature of its responsibilities to investigate violations of law within its investigative jurisdiction and ensure the internal security of the United States, collects information from a wide variety of sources. Basically, information is obtained, as a result of investigative efforts, from other Government agencies, law enforcement agencies, the general public, informants, witnesses, and public source material.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3), (d), (e)(1), (e)(2), and (H), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c), and (e).

[\[TOP\]](#)

System name:

FBI Counterdrug Information Indices System (CIIS).

System location:

The Department of Justice (DOJ) Computer Center, Rockville, Maryland, and at FBI Headquarters, Washington, DC.

Categories of individuals covered by the system:

Individuals who relate in any manner to official FBI drug law enforcement investigations including, but not limited to, subjects, suspects, victims, witnesses, and close relatives ; associates who are relevant to an investigation.

Categories of records in the system:

The records in the system will consist of automated indices to information located in drug enforcement case files of the FBI. Examples of the case files include those concerning distribution of controlled substances, continuing criminal enterprises, racketeering enterprises, Organized Crime Drug Enforcement Task Forces cases, and organized crime-drug intelligence cases.

These automated indices contain limited summary type data extracted from the case files. These indices will serve as a pointer system to FBI case files containing drug law enforcement information; but the system does not contain the case files themselves. Access to the case information must be gained by separate contact with the appropriate FBI office, outside the system, after the system has been queried. The system will facilitate better exchange of law enforcement information between and among the FBI and DEA, and such other law enforcement agencies as may participate in the counterdrug investigative information sharing program which this system serves.

Only specified data fields from these records will be provided. Examples of data fields include name, case file number, race, sex, name identifiers (alias, true-name, main, reference), individual, non-individual), locality indicators, date of birth, place of birth, ID numbers, addresses, violation codes, investigative classification, and office of origin. Data fields from

cases also include status, date case was opened, date case was closed, and point-of-contact information such as squad assigned, and auxiliary office. Additional point-of-contact information will be provided via a table of field offices and telephone numbers.

Authority for maintenance of the system:

Authority for this system is found at 28 U.S.C. 534, and 44 U.S.C. 3101.

Purpose(s):

The records in this system have been compiled for the purpose of identifying, apprehending and prosecuting individuals connected in any way with the manufacture, distribution, and use of illegal drugs. The system, by promoting the enhanced sharing of drug intelligence, is intended to facilitate enhanced cooperation between and among the FBI and DEA and other law enforcement agencies as may participate in the drug law enforcement information sharing program it serves, eliminate duplication of efforts, and enhance the safety of law enforcement personnel who conduct these inherently dangerous investigations.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

System records or any pertinent information derived therefrom may be disclosed (through electronic or other means in the case of participating Federal law enforcement agencies through other, non-electronic means as appropriate in other cases) to:

(1) Federal, state, local, and foreign law enforcement agencies, and components thereof support their role in the detection and monitoring of the distribution of illegal drugs in the United States or such other roles in support of counterdrug law enforcement as may be permitted by law; direct, electronic, "read only" access, by Federal law enforcement agencies only, to the automated indices of this system of records may enable these agencies to: identify FBI law enforcement information or activities which may be relevant to their law enforcement responsibilities and, where such information or activities are identified, request access to information in FBI case files relating to drug law enforcement, and (ii) ensure appropriate coordination of such activities with the FBI;

(2) Federal, state, local, and foreign law enforcement agencies, and components thereof to the extent necessary to elicit information pertinent to counterdrug law enforcement;

(3) Foreign law enforcement agencies with whom the FBI maintains liaison, and agencies of the U.S. foreign intelligence community to further the efforts of those agencies with respect to the national security and foreign affairs aspects of international drug trafficking;

(4) Individuals and organizations in the course of investigations to the extent necessary to obtain information pertinent to counterdrug law enforcement;

(5) Any person, organization, or entity within the private or public sector, domestic or foreign, to the extent necessary to prevent an imminent or potential crime which could or does directly threaten loss of life, serious injury, or serious loss of property;

(6) The news media and/or the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(7) A Member of Congress or staff acting upon the Member's behalf, when the Member requests the information on behalf of and at the specific request of the individual who is the subject of the record;

(8) National Archives and Records Administration and the General Services Administration records management inspections conducted under the authority of 44 U.S.C. 2904 and 2905;

(9) To a court or adjudicative body before which the FBI is authorized to appear when a party to the litigation is the following: (i) the FBI, or any subdivision thereof, or (ii) any employee of the FBI in his or her official capacity, or (iii) any employee of the FBI in his or her individual capacity where the DOJ has agreed to represent the employee, or (iv) the United States, where the FBI determines that the litigation is likely to affect it or any of its subdivisions.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or

official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records described in this system are stored on a mainframe computer at the DOJ Computer Center, and on back-up storage devices at FBI Headquarters, which are accessible by the DOJ.

Retrievability:

Information in the automated indices will be retrieved by name or other unique identifier. In addition to other Federal law enforcement agencies (reference routine use above), the law enforcement components of the DOJ may have direct, electronic, "read only" access (under subsection (b)(1) of the Privacy Act) to this system. This data will assist DOJ law enforcement components in identifying whether there may be detailed records which reside in the custody of the FBI that may be relevant to their law enforcement responsibilities. Where such records are identified, DOJ law enforcement components may request access to them.

Safeguards:

Access is limited to designated agency employees with a need-to-know. All records are kept in a secure area of a secure building. In addition to controlled access to the building, the area where records are kept are either attended by responsible employees, guarded by security personnel, and/or protected by electronic surveillance and/or alarm systems, as appropriate. In addition, unauthorized access to the automated indices is also prevented through state-of-the-art technology such as encryption and user ID's and multiple passwords.

Retention and disposal:

The automated indices in this system relate to case files which are characterized as either permanent or temporary, governed by NARA criteria in making such assessments. Depending on the nature of the case files to which they relate, the automated indices in this system are either retained permanently or disposed of in accordance with the FBI Records Disposition Schedule developed jointly by NARA and the FBI and approved by the United States District Court for the District of Columbia.

the District of Columbia, Washington, DC.

Systems manager(s) and address:

Director, Federal Bureau of Investigation, Washington, DC 20535.

Notification procedure:

Inquires should be addressed to: Federal Bureau of Investigation, Freedom of Information/Privacy Acts Section, 9th Street and Pennsylvania Avenue, NW, Washington 20535

Record access procedures:

Same as above.

Contesting records procedure:

Same as above.

Record source categories:

The data maintained in the automated indices in this system is derived from information drug law enforcement related case files, which are not part of this system.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c) (3) and (4), (d), (e) (2) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/FBI-017

System name:

National DNA Index System (NDIS).

System location:

Federal Bureau of Investigation: FBI Laboratory, U.S. Department of Justice, J. Edgar Hoover Building, 935 Pennsylvania Ave., NW., Washington, DC 20535-0001.

Categories of individuals covered by the system:

Individuals in this system include persons designated by criminal justice agencies as belonging to one or more of the following groups:

A. Convicted offenders: Persons who have been convicted of crimes in Federal, State, and local courts where the applicable law permits establishment of a DNA record for the convicted person.

B. Missing persons and their close biological relatives: Persons reported missing or whose whereabouts are unknown and sought and their close biological relatives, such as parents, siblings, and children.

C. Victims: Persons, living or dead, who have been victims of crimes where the perpetrator of the crime may have carried DNA of the victim away from the crime scene.

D. DNA personnel: Personnel in Federal, State, and/or local criminal justice agencies who perform duties related to or are responsible for DNA records.

Categories of records in the system:

The following definitions are used in this notice:

A. A DNA sample is a body tissue or fluid sample usually a blood and/or buccal sample that can be subjected to DNA analysis.

B. A DNA profile consists of a set of DNA identification characteristics, i.e., the particular chemical form at the various DNA locations (loci), which permit the DNA of one person to be distinguishable from that of another person.

C. A target DNA profile is a DNA profile submitted by a criminal justice agency for the purpose of identifying DNA profiles maintained by NDIS which match the target DNA profile.

D. A target DNA profile search is a search of appropriate NDIS DNA records for those records with DNA profiles that may match the target DNA profile.

E. Personally identifiable information is information such as names, dates of birth, or social security numbers which are normally used to identify individuals. Personally identifiable information, as used in this notice, does not include information derived from the examination of a DNA sample.

F. A DNA record includes the DNA profile as well as data required to manage and operate NDIS, i.e., the NDIS Agency identifier which serves to identify the submitting agency; the Specimen Identification Number; information related to the reliability and maintainability of DNA profiles; and names of the participating laboratories and DNA personnel associated with DNA profile analyses.

Records in this system do not include DNA samples but do include DNA profiles of persons described under "Categories of Individuals Covered by the System" in paragraph A–C. DNA records are input by criminal justice agencies for use by the NDIS. NDIS includes the names of DNA personnel associated with DNA profile analyses, the date after which DNA records given by a DNA analyst can be accepted, and, when applicable, the date after which associated DNA records are not accepted. NDIS does not contain case-related or other personally identifying information about the person from whom the DNA sample was collected.

DNA records are maintained as follows:

1. The Convicted Offender Index, consisting of DNA records from convicted offenders;
2. The Missing Persons Index, consisting of DNA records from missing persons;
3. The Close Biological Relatives Index, consisting of DNA records from close biological relatives of missing persons;
4. The Unidentified Persons Index, consisting of DNA records from recovered living persons (e.g., children who can't and others who can't or refuse to identify themselves), and records

dead persons (including their body parts and tissues), whose identities are not known;

5. The Victims Index, consisting of DNA records from victims, living or dead, from whom may have been carried away by perpetrators;

6. The Forensic Index, consisting of DNA records from persons whose identities are not with certainty and who left DNA at the scene of a crime or whose DNA was carried away and

7. The Population File, consisting of DNA profiles intended to represent various population segments found in the United States. The Population File consists of DNA records from individuals whose identities may be: (a) Known to; (b) not known, but determinable under some circumstances by; or (c) not known and not determinable by the criminal justice agency submitting the DNA records to NDIS.

Authority for maintenance of the system:

The Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796.

Purpose(s):

The purpose of this system and the DNA records maintained in the system is to provide a national storage medium for DNA records input by criminal justice agencies. These records may be searched in order to identify DNA associations with a DNA record obtained during an investigation of a crime or a missing person. The system is also maintained for statistical identification research, and protocol development and quality control purposes.

In addition to DNA records, records about DNA personnel are maintained in the system. The purposes of these DNA personnel records are to control the acceptance of DNA records into NDIS and to facilitate criminal justice agency contracts required to resolve potential DNA matches.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

1. Direct disclosures of NDIS records are made to the Federal, State, and local criminal

agencies who participate in NDIS. As a result of an NDIS search by a criminal justice agency, the NDIS system analyzes the target DNA profile entered by the search agency and may identify a potential match. Where NDIS identifies a potential match, the matching DNA's records will be disclosed to the criminal justice agencies associated with the match.

2. The Federal statute which authorizes NDIS also provides that the FBI and other criminal justice agencies participating in NDIS may make secondary or indirect disclosures of DNA records:

- (A) To criminal justice agencies for law enforcement identification purposes;
- (B) In judicial proceedings, if otherwise admissible pursuant to applicable statutes or rules;
- (C) For criminal defense purposes, to a defendant, who shall have access to samples and analyses performed in connection with the case in which defendant is charged; or
- (D) If personally identifiable information is removed, for a population statistics database, identification research and protocol development purposes, or for quality control purposes.

Note:

Personal information such as names are not found in NDIS. However, operational identifiers such as the Specimen No., Criminal Justice Agency Identifier, and DNA Personnel identifiers are contained in NDIS. Although unlikely, the identity of an individual could, under some circumstances, be ascertained with the disclosure of such numbers for purposes stated above. This is only possible when access to a criminal justice agency's records is provided to the holder of the operational identifiers. Therefore, to ensure that such associations are not made, these operational numbers will be removed before disclosure for these purposes.

3. A record may be disclosed from this system of records to the National Archives and Records Administration and the General Services Administration in records management inspection conducted under the authority of 44 U.S.C. 2904 and 2906, to the extent that legislation governing the records permits.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes

responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in NDIS is stored electronically for use in a computer environment.

Retrievability:

The primary method for retrieving information from NDIS is the target DNA profile search described in the routine use disclosure provisions of this notice.

The NDIS Custodian may retrieve records based on: the DNA profile, the NDIS Agency identifier, the NDIS Specimen Identification Number, and/or DNA personnel identifier. Criminal justice agencies with direct access to NDIS may retrieve their records by the NDIS Agency identifier, NDIS Specimen Identification Number, or DNA personnel identifier but only to inspect, modify, or delete their own DNA records.

Since NDIS records contained in NDIS do not include personal identifiers of the individual from whom the DNA samples were collected, retrieval by personal identifiers of these records for the subjects is not possible.

Safeguards:

All records in NDIS are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include restricting access to those with a need-to-know to perform their official duties, using locks and alarm devices, and encrypting data communications.

No personally identifiable information about individuals who provided DNA samples is maintained in NDIS. Therefore, names and personally identifiable information of NDIS C

records cannot be disclosed directly from NDIS. (NDIS does, however, maintain the names of NDA personnel.)

NDIS will disclose to a criminal justice agency the DNA records of another criminal justice agency only when there is a potential DNA match. Any additional disclosures of personally identifiable information or other case-related data are made directly by the criminal justice agencies from their own files and records, not from NDIS.

Although ostensibly devoid of personally identifiable information, DNA records in NDIS contain an NDIS Specimen Identification Number, NDIS Agency identifier, and a DNA personnel identifier for law enforcement and/or general operational purposes. Since it is possible, under certain circumstances, to use those numbers together with the appropriate agency's own records to identify the individuals represented by the DNA records, additional precautions are taken.

The precautions involve removal of the Specimen Identification Numbers, NDIS Agency identifiers, and DNA personnel identifiers, prior to disclosure pursuant to the 2(D) routine use. (See the "Routine Uses of Records Maintained in the System" section of this notice.) The NDIS will periodically generate DNA profile data sets, consisting of anonymous DNA profiles for population statistics databases, for identification research and protocol development purposes, or for quality control purposes.

Criminal justice agencies are prohibited from submitting a DNA record for inclusion in the Population File for investigative purposes. The only target DNA profile searches conducted against the Population File are those necessary to eliminate duplicate DNA profiles representing the same individual.

Finally, criminal justice agencies with direct access to NDIS must agree to adhere to national quality assurance standards for DNA testing, undergo semi-annual external proficiency testing, and restrict access to DNA samples and data. The NDIS will not accept DNA analyses from those agencies and/or DNA personnel who fail to comply with these standards and restrictions, and the NDIS Custodian is authorized to restrict access to and delete any DNA records previously entered into the system.

Retention and disposal:

DNA records generated by criminal justice agencies, together with the personal identifying information of DNA personnel, shall be retained in NDIS as long as they are substantiated.

internal records of the submitting agency and are permitted either by consent, by judicial/criminal justice authority, or by Federal, State, or local law. Records may be deleted from the originating criminal justice agency or by other Federal, State, or local authorities who are responsible for deleting any records that are no longer permitted or appropriate for retention in NDIS. DNA records submitted to NDIS and then found to be inaccurate shall either be corrected to achieve accuracy or deleted from NDIS by the submitting agency.

Agencies granted access to NDIS are required to establish and maintain a system of controls to ensure that continued use of their DNA records in NDIS is lawfully permitted. Such a system of controls shall ensure that DNA records in NDIS which are authorized by the consent of individuals, for example, are retained in NDIS only for the duration and within the scope of the consent.

The NDIS Custodian has the authority to determine that certain DNA records in NDIS shall be deleted or, alternatively, suspended from use for a period of time determined appropriate by the NDIS Custodian. The criminal justice agencies whose records are affected by a determination to delete or suspend records in NDIS shall be notified of this determination and the nature of the deletion or suspension. The NDIS Custodian may subsequently decide to either restore or delete the suspended records, and shall notify the affected agency of the subsequent determination.

The DNA personnel identifier for a single individual is deleted from NDIS only after all DNA records associated with that individual are deleted.

System manager(s) and address:

Director, Federal Bureau of Investigation, c/o National DNA Index System Custodian, FBI Laboratory, U.S. Department of Justice, J. Edgar Hoover Building, 935 Pennsylvania Avenue NW., Washington, DC 20535-0001.

Notification procedure:

None. This system of records has been exempted from subsections (d) and (e)(4)(G) pursuant to subsection (j)(2) of the Privacy Act, and thus is exempt from the notification provision.

Records access procedure:

This system of records has been exempted from subsection (d) and (e)(4)(H) pursuant to subsection (j)(2) of the Privacy Act, and thus is exempt from its access provisions. NDIS does not retain information that would allow the NDIS Custodian, independent of the agency that originated the DNA record, to personally identify the record by name or other personal identifier. However, subject to applicable Federal, State, and local law and procedures, the following alternative procedures are available by which an individual may request access to records in NDIS.

1. Subjects of DNA Records:

a. **Convicted Offender Records:** The individual may contact the Federal, State or local agency (the authorized agency) which ultimately received the collected DNA sample to obtain instructions on how to access his/her record. The authorized agency has the DNA record if one exists, including information as to whether the DNA record has been submitted to NDIS. Only the authorized agency would have information sufficiently specific to permit retrieval of the record from its files by name or other personally identifiable information. The authorized agency may also retrieve the DNA record, if any, that was submitted to NDIS, once locally specified requirements are met.

In addition, where a convicted offender is relocated voluntarily or involuntarily to a criminal justice agency (i.e., penal institution or parole and probation authorities) for custodial or supervisory purposes in another State or jurisdiction, the DNA record may be created by the new host criminal justice agency or other State (or Federal) authority from a DNA sample collected from the Convicted Offender at the new host criminal justice agency or other State (or Federal) authority. In such circumstances, the individual may contact such agency or authority for access instructions.

b. **Close Biological Relatives of Missing Persons and Victims; Living Victims; and Missing Persons Who Have Been Located:** These individuals must contact the criminal justice agency (Federal, State, or local) which collected and processed the DNA sample to generate the DNA record. The criminal justice agency can then advise the individual about procedures for accessing the DNA record. Such agency may also retrieve the DNA record, if any, that was submitted to NDIS, once locally specified requirements are met.

2. **Records of DNA Personnel:** These individuals may write to the Federal, State, or local criminal justice agency by which they are or were employed.

3. FBI generated records: The subject of an FBI-generated DNA record may address a Freedom of Information/Privacy Act (FOIA/PA) request to the Director, FBI, at the address at the end of this paragraph. DNA personnel employed by the FBI may also address the requests to the system manager; however, all the information in NDIS concerning DNA personnel is also contained in the FBI's Central Records System (CRS), which may contain additional information. To request access to the CRS, DNA personnel may address an FOIA/PA request to the Director, FBI, U.S. Department of Justice, J. Edgar Hoover Building, 935 Pennsylvania Ave., NW., Washington, DC 20535-0001.

Contesting records procedure:

This system of records has been exempted from subsections (d) and (e)(4)(H) pursuant to subsection (j)(2) of the Privacy Act, and is thus exempt from its amendment and correction provisions. However, subject to applicable Federal, State, and local laws and procedures, following alternative procedures are available by which an individual may contest his/her records:

1. All Subjects of DNA Records: The requester must follow the same procedures for correcting records as those outlined under "Record Access Procedures." In addition, the requester must be aware of the following:

a. DNA records submitted to NDIS and contested on the basis of inaccurate information must be resolved with the criminal justice agency that submitted the DNA record to NDIS. If a contested DNA record is found to be inaccurate by the criminal justice agency submitting the DNA record, such agency shall correct the inaccurate DNA record by either amending or deleting the record.

b. DNA records submitted to NDIS and contested on the basis of the authority to retain a DNA record must be resolved with the criminal justice agency that submitted the contested DNA record. If such agency determines that the contested DNA records should not be in NDIS, such agency must delete the contested DNA record.

2. Records of All DNA Personnel: DNA personnel must follow the same procedures for contesting records as those outlined under "Record Access Procedures."

Record source categories:

DNA records in NDIS are received from Federal, State, and local criminal justice agencies. These DNA records may be derived from DNA samples obtained by Federal, State, and local criminal justice agencies or their agents (public or private).

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system of records from subsection (c) (3) and (e) (1), (2), and (3); (e)(4) (G) and (H); (e) (5) and (8); and (g) of the Privacy Act pursuant to U.S.C. 552a(j)(2). Rules are being promulgated in accordance with the requirements of U.S.C. 553 (b), (c), and (e); and are being published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/FBI-018

System name:

National Instant Criminal Background Check System (NICS).

System location:

Federal Bureau of Investigation, 1000 Custer Hollow Road, Clarksburg, West Virginia 26301

Categories of individuals covered by the system:

The categories of individuals covered by the system include any person who:

- A. Is under indictment for, or has been convicted in any court of, a crime punishable by imprisonment for a term exceeding one year;
- B. Is a fugitive from justice;
- C. Is an unlawful user of or addicted to any controlled substance;
- D. Has been adjudicated as a mental defective or has been committed to a mental institution;
- E. Is an alien who is illegally or unlawfully in the United States or who has been admitted to the United States on a temporary lawful basis.

United States under a non-immigrant visa;

F. Has been discharged from the Armed Forces under dishonorable conditions;

G. Having been a citizen of the United States, has renounced such citizenship;

H. Is subject to a court order that restrains the person from harassing, stalking, or threatening an intimate partner or child of such intimate partner (issued after a hearing of which actual notice was received);

I. Has been convicted in any court of a misdemeanor crime of domestic violence (involving the use or attempted use of physical force committed by a current or former spouse, parent, or guardian of the victim or by a person with a similar relationship with the victim);

J. Is otherwise disqualified from possessing a firearm under State law;

K. Is for claims to be a Federal firearms licensee (FFL), i.e., a person licensed by the Bureau of Alcohol, Tobacco and Firearms (ATF), United States Department of Treasury, as a manufacturer, dealer, or importer of firearms; or

L. Has applied for the transfer of a firearm or for a firearms-related permit or license and had his or her name forwarded to the NICS as part of a request for a NICS background check. (Identifying information about this category of individuals is maintained for system administration and security purposes in the "NICS Audit Log," a system transaction log described below under the headings "CATEGORIES OF RECORDS IN THE SYSTEM" and "RETENTION AND DISPOSAL." Identifying information may also be maintained in appeals for those individuals who have requested the reason for a denial or delay from the FBI, a law enforcement agency serving as a POC, and/or challenged the accuracy or validity of a disqualifying record or otherwise inquired about a NICS transaction. In cases of allowed transfers, all information in the NICS Audit Log related to the person or the transfer, other than the NICS Transaction Number (a unique number assigned to each valid background check inquiry) assigned to the transfer and the date the number was assigned, will be destroyed not more than 90 days after the transfer is allowed, provided that such information may be retained for a longer period if necessary to pursue identified cases of misuse of the system. In such cases, the system will not contain any details about the type of firearm which is the subject of the proposed transfer (other than the fact that it is a handgun or long gun) or

whether a sale or transfer of a firearm has actually taken place.)

Categories of records in the system:

The "NICS Index" is the only database maintained by the FBI which was created specifically for the NICS. The NICS Index contains records obtained by the Attorney General from Federal agencies or States on individuals who fall into the categories of individuals listed above under the heading "CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM," C through H. These records contain an individual's name; sex; race; other personal descriptive data (including scars and tattoos); complete date of birth; state of residence; sometimes a unique identification number, such as a Social Security number (but NICS does not require it to be furnished); military number, or a number assigned by Federal, State, or local law enforcement authority.

The "NICS Audit Log" is a chronological record of system (computer) activities that enable reconstruction and examination of a sequence of events and/or changes in an event relating to the NICS. With regard to a specific NICS transaction, the audit log will include: The name of the individual; other identifying information about the prospective transferee; the type of transaction (inquiry or response); line number; time; date of inquiry; header; message key; Originating Agency Identifier; and inquiry/response data, such as a NICS Transaction Number (a unique number assigned to each valid background request inquiry) and information found by the NICS.

In addition, the NICS contains information on persons that are FFLs (or claim to be). This information includes the FFL name, address, phone numbers, ATF number, access code, keywords, names of authorized representatives and contact persons, and similar information used by the NICS to identify, validate, and communicate with FFLs in the course of NICS operations.

The NICS also contains "appeals records" which reflect inquiries by individuals regarding the reason for a delay or denial by the FBI or a POC, and/or challenges to the accuracy or validity of a disqualifying record, or other types of inquiries made by individuals about a NICS transaction.

Authority for maintenance of the system:

(1) 18 U.S.C. 922, as amended by the Brady Handgun Violence Prevention Act (the "Brady Act") (Pub. L. 103-159, Nov. 30, 1993); (2) 28 U.S.C. 534, as amended (Pub. L. 103-322, IV, 4060(a), Sep. 13, 1994, 105 Stat. 1950).

Purpose(s):

The purpose of the NICS, which was established pursuant to the Brady Act, is to provide means of checking available information to determine whether a person is disqualified from possessing a firearm under Federal or State law.

Prior to the transfer of a firearm, a prospective transferee, not licensed under 18 U.S.C. must obtain a firearms transaction form from an FFL and provide the information required by the ATF. The firearms transaction form is returned to the FFL, who is required by the Brady Act to contact the NICS and furnish the name and certain other identifying data provided by the transferee. NICS conducts a search which compares the information about the transferee with information in or available to NICS.

State and local law enforcement agencies may serve as Points of Contact (POCs) for the NICS. Where there is no POC, the FBI's NICS Operations Center serves in its place. The POC (NICS Operations Center) receives inquiries from FFLs, initiates NICS background search, may check available state and local record systems, determines whether matching records exist, may provide information demonstrating that an individual is disqualified from possessing a firearm under Federal or State law, and responds back to the FFLs.

In addition to a review of the NICS Index, a NICS search includes a review of the pre-existing, separately-managed FBI criminal history databases of the National Crime Information Center (NCIC)(JUSTICE/FBI-001), including the Interstate Identification Index (III), to the extent searches are possible with the available information. NCIC and III are cooperative Federal programs for the exchange of criminal history record and other information among criminal justice agencies to locate wanted and missing persons and for other identification purposes. The search conducted of the NCIC and III, in conjunction with the search of the NICS Index, attempts to locate only information indicating that an individual firearm transferee is identical to an individual in one or more of categories A through J listed above under the heading CATEGORIES OF INDIVIDUALS IN THE SYSTEM, with the search of NCIC and III specifically directed towards locating information that an individual is within categories A, B, C, D, F,

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The FBI may disclose relevant system records to the following persons or entities under

circumstances or for the purposes described below, to the extent such disclosures are compatible with the purpose for which the information was collected. (Routine uses are meant to be mutually exclusive and may overlap in some cases.)

A. Limited information may be provided by a POC or the NICS Operations Center to an individual who has contacted the NICS concerning a prospective firearm transferee. If a matching record is found by the NICS provides information demonstrating that the prospective transferee is disqualified from possessing a firearm under Federal or State law, the FFL will be notified that the application is "denied," with none of the underlying information provided. If additional record analysis is required by the NICS representative (e.g. to confirm that a record relates to the potential transferee or to pursue supplemental information to clarify whether the potential transferee is disqualified from receiving a firearm), the response may read "delayed" and include an estimated time for completing the analysis. If no disqualifying record is located in the NICS, the FFL will be told that it may "proceed." A unique identification number will be provided to the FFL for all responses received from the NICS, which number shall be recorded on the firearms transaction form.

B. Information in the NICS may be provided through the NCIC lines to Federal criminal justice agencies, criminal justice agencies in the fifty States, the District of Columbia, Puerto Rico, U.S. Possessions, and U.S. Territories, including POCs and contributors of information to the NICS Index, to enable them to determine whether the transfer of a firearm to any person licensed under 18 U.S.C. 923 would be in violation of Federal or State law; whether the issuance of a license or permit for the possession or sale of a firearm or firearms, or to carry a concealed firearm, or to import, manufacture, deal in, or purchase explosives would be in violation of Federal or State law or regulation; whether appeals from denials should be granted or denied; and whether to add to, delete from, revise, or update information previously provided by the contributor. This includes responding to inquiries by the ATF in connection with enforcement of the Gun Control Act (18 U.S.C. Chapter 44), or the National Firearms Act (18 U.S.C. Chapter 53).

C. If, during the course of any activity or operation of the system authorized by the regulation governing the system (28 CFR, part 25, subpart A), any record is found by the system which indicates, either on its face or in conjunction with other information, a violation or potential violation of law (whether criminal or civil) and/or regulation, the pertinent record may be disclosed to the appropriate agency/organization/task force (whether Federal, State, local, joint, or tribal) and/or to the appropriate foreign or international agency/organization charged with the responsibility of investigating, prosecuting, and/or enforcing such law or regulation.

e.g., disclosure of information from the system to the ATF, United States Department of Treasury, regarding violations or potential violations of 18 U.S.C. 922(a)(6). (This routine does not apply to the NICS Index.)

D. System records may be disclosed to contractors, grantees, experts, consultants, volunteers, detailees, and other non-FBI employees performing or working on a contract, service, grant, cooperative agreement, or job for the Federal Government when necessary to accomplish an agency function related to this system of records and under requirements (including Privacy Act requirements) specified by the FBI.

E. System records may be disclosed to the news media or members of the general public to assist a victim or potential victim in furtherance of a legitimate law enforcement or public safety function, e.g., to assist in locating fugitives; to provide notification of arrests; to provide assessments, or similar information on potential threats to life, health, or property; or to inform the public appropriately informed of other law enforcement or FBI matters of legitimate public interest. (The availability of information in pending criminal cases will be governed by the provisions of 28 CFR 50.2.) (This routine use does not apply to the NICS Index.)

F. Where the disclosure of system records has been determined by the FBI to be reasonable and necessary to resolve a matter in litigation or in anticipation thereof, such records may be disclosed to a court or adjudicative body, before which the FBI is authorized to appear, (a) The FBI or any FBI employee in his or her official capacity; (b) any FBI employee in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (c) the United States, where the FBI determines it is likely to be affected by the litigation or could be a party to the litigation, or has an official interest in the litigation.

G. System records may be made available to a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information on behalf and at the written request of the individual who is the subject of the record.

H. System records may be disclosed to the National Archives and Records Administration for records management inspections and such other purposes conducted under the authority of 44 U.S.C. 2904 and 2906.

I. Information pertaining to individuals who have been denied a firearm by the NICS may be disclosed, either electronically or otherwise, to a federal, state, local, joint, tribal, foreign, international, or other public agency/organization where such disclosure may promote,

or otherwise serve law enforcement interests. By way of example and not limitation, such disclosures may, for instance, include posting all NICS denials on a centralized database that would be electronically accessible to law enforcement agencies.

J. Information in the NICS Audit Log (including records of approved and denied transfers) may be disclosed to the Bureau of Alcohol, Tobacco, and Firearms (ATF) in connection with inspections of Federal Firearms Licensee records.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are stored electronically for use in a computer environment in areas safe from unauthorized access by unauthorized persons or exposure to environmental hazards. In general, the security standards for the NCIC (JUSTICE/FBI-001) is followed.

Retrievability:

Records are retrieved by name, sex, race, date of birth, state of residence, other personal descriptive data, the NICS Transaction Number, FFL number, and, in some instances, a unique numeric identifier, e.g., a Social Security number or a military identification number. (A Social Security number is not required by the NICS.)

Safeguards:

Records searched by the NICS are located in secure government buildings with limited physical access. Access to the results of a NICS record search is further restricted to authorized employees of Federal, State, and local law enforcement agencies who make

inquiries by use of identification numbers and code words.

When a Federal, State, or local agency places information in the NICS Index, it uses its identifier and a unique agency record identifier for each record provided to the NICS. Federal, State, or local agencies can modify or cancel only the data that they have provided to the NICS Index.

Retention and disposal:

Information provided by other Federal agencies or State or local governments will be maintained in the NICS Index unless updated or deleted by the agency/government which contributed the data.

The FBI will maintain an audit Log of all NICS transactions. Firearms transaction approval information will be maintained for 90 days (except that such information may be retained for a longer period as necessary to pursue identified cases of misuse of the system). The NICS Transaction Number (the unique number assigned to the NICS transaction) and the date on which it was assigned will be maintained indefinitely. Information related to firearms transfer denials will be retained for 10 years and then disposed of as directed by the National Archives and Record Administration.

System manager(s) and address:

Director, Federal Bureau of Investigation, J. Edgar Hoover FBI Building, 935 Pennsylvania Avenue, NW, Washington, DC 20535-0001.

Notification procedure:

This system of records has been exempted from the notification procedures of subsection (e)(4)(G), to the extent permitted by subsections (j)(2), (k)(2), and (k)(3) of the Privacy Act. Requests for notification should be addressed to the Systems Manager. Requirements for notification request are the same as set forth below under the heading "RECORD ACCESS PROCEDURES."

Record access procedures:

This system of records has been exempted from the access procedures of subsections

(e)(4)(H) to the extent permitted by subsections (j)(2), (k)(2), and (k)(3) of the Privacy Act request for access to a non-exempt record from the system should be addressed to the System Manager, shall be made in writing, and should have the envelope and the letter marked "Privacy Act Request." The request must include the full name, complete address, date of birth, and place of birth of the requester. The requester must sign the request; to verify it, the signature must be notarized or submitted under 28 U.S.C. 1746, a law that provides statements to be made under penalty of perjury as a substitute for notarization.

Alternative procedures are available to a person who has been denied the transfer of, or for, a firearm or explosives because of information in the NICS. The procedures provide an appeal of a denial and a method to seek the correction of erroneous data searched by or maintained in the system. The alternative procedures can be found at 28 CFR, part 25, subpart A.

Contesting record procedures:

This system of records has been exempted from the contest and amendment procedures of subsections (d) and (e)(4)(H) to the extent permitted by subsections (j)(2), (k)(2), and (k)(3) of the Privacy Act. Requests should be addressed to the System Manager and should clearly and concisely describe the precise information being contested, the reasons for contesting it, and the proposed amendment or correction proposed to the information. In addition, as described above under "RECORD ACCESS PROCEDURES," an alternative procedure is available to a person who has been denied the transfer of, or permit for, a firearm or explosives because of information in the NICS, by which the individual may seek the correction of erroneous data in the system. The procedures are further described at 28 CFR, part 25, subpart A.

Record source categories:

Information contained in the NICS is obtained from local, State, Federal, and international records.

System exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d); (e)(4)(G) and (H); (e)(5) and (8); and (g) of the Privacy Act, pursuant to 5 U.S.C. 552a(j)(2). In addition, the Attorney General has exempted this system from subsections (d), (e)(1), and (e)(4)(G) and (H) of the Privacy Act, pursuant to 5 U.S.C. 552a (k)(2) and

Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), and (e), and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/FBI-019

System name:

Terrorist Screening Records System (TSRS).

Security classification:

Classified, unclassified (law enforcement sensitive).

System location:

Records described in this notice are maintained at the Terrorist Screening Center, Federal Bureau of Investigation, Washington, D.C., and at facilities operated by other government entities for terrorism screening, system back-up, and continuity of operations purposes.

Categories of individuals covered by the system:

- a. Individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism ("known or suspected terrorists");
- b. Individuals who are the subject of queries against TSC information systems;
- c. Individuals identified during a terrorism screening process as a possible identity match to a known or suspected terrorist and other individuals who accompany or travel with such individuals;
- d. Individuals who are misidentified as a possible identity match to a known or suspected terrorist ("misidentified persons");
- e. Individuals about whom a terrorist watchlist-related redress inquiry has been made; a

f. Individuals whose information is collected and maintained for information system user auditing and security purposes, such as individuals who are authorized users of TSC information systems.

Categories of records in the system:

a. Identifying information, such as name, date of birth, place of birth, biometrics, photograph and/or drivers license information, and other available identifying particulars used to compare the identity of an individual being screened with a known or suspected terrorist, including audit records containing this information;

b. Information about encounters with individuals covered by this system, such as date, location, screening entity, analysis, associated individuals, and results (positive or negative identity match), and, for encounters with known or suspected terrorists only, other entities notified and details of any law enforcement, intelligence, or other operational response;

c. For known or suspected terrorists, in addition to the categories of records listed above, references to and/or information from other government law enforcement and intelligence databases, or other relevant databases that may contain terrorism information;

d. For misidentified persons, in addition to the categories of records listed above, additional identifying information that will be used during screening only for the purpose of distinguishing them from a known or suspected terrorist who has similar identifying characteristics (such as name and date of birth);

e. For redress matters, in addition to the categories of records listed above, information provided by individuals or their representatives, information provided by the screening agency and internal work papers and other documents related to researching and resolving the matter;

f. Information collected and compiled to maintain an audit trail of the activity of authorized users of TSC information systems, such as user name/ID, date/time, search query and results, data, user activity information (e.g., record retrieval, modification, or deletion data), and unique identifiers;

g. Archived records and record histories from the Terrorist Screening Database, Encouragement Management Application, and other TSC data systems that are part of the TSRS.

Authority for maintenance of the system:

Homeland Security Presidential Directive-6, "Integration and Use of Screening Information to Protect Against Terrorism" (Sept. 16, 2003); Executive Order 13388, Further Strengthen Sharing of Terrorism Information to Protect Americans," (October 25, 2005); the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458; the National Security Act of 1947, as amended; and 28 U.S.C. 533. In the event that the TSC's continuity-of-operation plans are invoked, the agency that assumes TSC operational functions will have the authority to administer the Terrorist Screening Records System as necessary to carry out those functions.

Purpose(s):

- a. To implement the U.S. Government's National Strategy for Homeland Security and Homeland Security Presidential Directive-6, to identify potential terrorist threats, to uphold and enforce the law, and to ensure public safety.
- b. To consolidate the government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes.
- c. To maintain current, accurate and thorough terrorist information in a consolidated terrorist screening database and determine which terrorism screening processes will use each element of the database.
- d. To ensure that appropriate information possessed by State, local, territorial, and tribal governments, which is lawfully available to the Federal Government, is considered in determinations made by the TSC as to whether a person is a match to a known or suspected terrorist.
- e. To host mechanisms and make terrorism information available to support appropriate domestic, and foreign terrorism screening processes, and private-sector screening processes that have a substantial bearing on homeland security.
- f. To provide continual operational support to assist in the identification of persons screened and to facilitate an appropriate and lawful response when a known or suspected terrorist is identified in an authorized screening process.

- g. To provide appropriate government officials, agencies, or organizations with information about encounters with known or suspected terrorists.
- h. To assist persons misidentified during a terrorism screening process and to assist such agencies or entities in responding to individual complaints about the screening process (redress).
- i. To oversee the proper use, maintenance, and security of TSC data systems and TSC personnel.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, the records or information in this system may be disclosed as a routine use, under 5 U.S.C. 552a(b)(3), in accordance with blanket routine uses established for FBI record systems. Blanket Routine Uses (BRU) Applicable to More Than One FBI Privacy Act System of Records: Justice/FBI-BRU, published on June 22, 2001 at 66 FR 33558 and amended on February 2, 2005 at 70 FR 7513. In addition, as routine uses specific to this system, the TSC may disclose relevant system records to the following persons or entities and under the circumstances and for the purposes described below, to the extent such disclosures are compatible with the purposes for which the information was collected. (Routine uses are not meant to be mutually exclusive and may overlap in some cases.)

A. To those federal agencies that have agreed to provide support to TSC for purposes consistent with ensuring the continuity of TSC operations.

B. To federal, state, local, tribal, territorial, foreign, multinational or other public agency or entities, to entities regulated by any such agency or entity, and to owners/operators of critical infrastructure or private sector entities with a substantial bearing on homeland security and their agents, contractors or representatives, for the following purposes: (1) For use in and support of terrorism screening authorized by the U.S. Government, (2) to provide appropriate notifications of the results of terrorism screening using information from the Terrorist Screening Database or a threat related to a positive encounter with an individual identified in the Terrorist Screening Database, (3) to facilitate any appropriate law enforcement or other response (including medical and containment response to a biological hazard) to a known or suspected terrorist.

a threat related to the encounter, and (4) to assist persons misidentified during a screening process.

C. To any person, organization, or governmental entity in order to notify them of a serious terrorist threat for the purpose of guarding against or responding to such a threat.

D. To federal, state, local, tribal, territorial, foreign, or multinational agencies or entities, other organizations that are engaged in, or are planning to engage in terrorism screening authorized by the U.S. Government, for the purpose of the development, testing, or modification of information technology systems used or intended to be used during or in support of the screening process; whenever practicable, however, TSC, to the extent possible, will substitute anonymized or de-identified data, such that the identity of the individual cannot be derived from the data.

E. To federal, state, local, tribal, territorial, foreign, multinational agencies or entities, or sector entities to assist in coordination of terrorist threat awareness, assessment, analysis, and response.

F. To any person or entity in either the public or private sector, domestic or foreign, where reasonably necessary to elicit information or cooperation from the recipient for use by the TSC in the performance of an authorized function, such as obtaining information from data sources, as to the thoroughness, accuracy, currency, or reliability of the data provided so that the TSC may review the quality and integrity of its records for quality assurance or redress purposes and may also assist persons misidentified during a screening process.

G. To any federal, state, local, tribal, territorial, foreign or multinational agency, task force, or other entity or person that receives information from the U.S. Government for terrorism screening purposes, in order to facilitate TSC's or the recipient's review, maintenance, and correction of TSC data for quality assurance or redress purposes, and to assist persons misidentified during a screening process.

H. To any agency, organization or person for the purposes of (1) performing authorized security, audit, or oversight operations of the DOJ, FBI, TSC, or any agency, organization, or person engaged in or providing information used for terrorism screening that is supported by the TSC, and (2) meeting related reporting requirements.

I. To a former employee of the TSC or a former contractor supporting the TSC for purposes

Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with any applicable government regulations; or facilitating communications with a former employee/contractor that may be necessary for personnel-related or other official purposes where the TSC requires information and/or consultation/assistance from the former employee/contractor regarding a matter within that person's area of responsibility.

J. To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, tribal, multinational or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

K. To a governmental entity lawfully engaged in collecting law enforcement, law enforcement intelligence, national security information, national intelligence, or terrorism information/enforcement, intelligence, or counterterrorism purposes.

L. To appropriate agencies, entities, and persons when (1) the Department of Justice suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department of Justice has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems/programs (whether maintained by the Department or another agency or entity) that rely on the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department of Justice's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy the harm.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records in this system are stored in paper and/or electronic format. Electronic storage includes servers, CD-ROMs, DVD-ROMs, and magnetic tapes.

Retrievability:

Records in this system are typically retrieved by individual name, date of birth, passport number, and other identifying data, including unique identifying numbers assigned by t or other government agencies.

Safeguards:

All records are maintained in a secure government facility with access limited to only au personnel or authorized and escorted visitors. Physical security protections include gua locked facilities requiring badges and passwords for access. Records are accessed only authorized government personnel and contractors and are protected by appropriate phy and technological safeguards to prevent unauthorized access. All Federal employees a contractors assigned to the TSC must hold an appropriate security clearance, sign a non-disclosure agreement, and undergo privacy and security training.

Retention and disposal:

Records in this system will be retained and disposed of in accordance with the records schedule approved by the National Archives and Records Administration. For records maintained in the Terrorist Screening Database, active records are maintained for 99 ye inactive (archived) records are maintained for 50 years. Records of possible encounters individuals on the Terrorist Screening Database are maintained for 99 years. Records of redress inquiries and quality assurance matters are maintained for at least six years. Au are maintained for 25 years and records of user audits are maintained for ten years.

System manager(s) and address:

Director, Terrorist Screening Center, Federal Bureau of Investigation, FBI Headquarters
Pennsylvania Avenue, NW., Washington, DC 20535-0001.

Notification procedure:

Because this system contains classified intelligence and law enforcement information re the government's counterterrorism, law enforcement, and intelligence programs, record system have been exempted from notification, access, and amendment to the extent pe by subsections (j) and (k) of the Privacy Act.

Requests for notification should be addressed to the FBI at the address and according to requirements set forth below under the heading "Record Access Procedures."

Record access procedures:

Because this system contains classified intelligence and law enforcement information related to the government's counterterrorism, law enforcement and intelligence programs, records in this system have been exempted from notification, access, and amendment to the extent permitted by subsections (j) and (k) of the Privacy Act. A request for access to a non-exempt record may be made in writing with the envelope and the letter clearly marked "Privacy Act Request." Include in the request your full name and complete address. The requester must sign the request; and, to verify it, the signature must be notarized or submitted under 28 U.S.C. 1792, a law that permits statements to be made under penalty of perjury as a substitute for notarization. You may submit any other identifying data you wish to furnish to assist in making a proper search of the system. Requests for access to information must be addressed to the Record Information Dissemination Section, Federal Bureau of Investigation, 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001.

Contesting record procedures:

Because this system contains classified intelligence and law enforcement information related to the government's counterterrorism, law enforcement and intelligence programs, records in this system are exempt from notification, access, and amendment to the extent permitted by subsections (j) and (k) of the Privacy Act (5 U.S.C. 552a). Requests for amendment should be addressed to the FBI at the address and according to the requirements set forth above under the heading "Record Access Procedures."

If, however, individuals are experiencing repeated delays or difficulties during a government screening process and believe that this might be related to a terrorist watch list entry, they may contact the Federal agency that is conducting the screening process in question ("screening agency"). The screening agency is in the best position to determine if a particular problem relates to a terrorist watch list entry or is due to some other cause, such as a criminal history, an immigration violation or random screening. Some individuals also experience repeated delays during screening because their names and/or other identifying data, such as dates of birth, are similar to those of known or suspected terrorists. These individuals, referred to as "misidentified persons," often believe that they themselves are on a terrorist watch

when in fact they only bear a similarity in name or other identifier to an individual on the Most screening agencies have or are developing procedures to expedite the clearance of misidentified persons during screening.

By contacting the screening agency with a complaint, individuals will be able to take advantage of the procedures available to help misidentified persons and others experiencing screening problems. Check the agency's requirements for submitting complaints but, at a minimum, individuals should describe in as much detail as possible the problem they are having, including dates and locations of screening, and provide sufficient information to identify themselves, such as full name, citizenship status, and date and place of birth. The TSC is the screening agency in resolving any screening complaints that may relate to terrorist watch list information, but does not receive or respond to individual complaints directly. However, if TSC receives any such complaints, TSC will forward them to the appropriate screening agency.

Additional information about the redress process and how to file a complaint with a screening agency is available on TSC's Web site at <http://www.fbi.gov/terrorinfo/counterrorism/redress.htm>.

Record Source Categories:

Information in this system is obtained from individuals covered by the system, public social media agencies and private sector entities conducting terrorism screening, law enforcement and intelligence agency record systems, government databases, and foreign governments.

Exemptions Claimed for the System:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d)(1), (2), (3), (5) and (8), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(k). These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e).

[\[TOP\]](#)

JUSTICE/FBI-020

System Name:

Law Enforcement National Data Exchange (N-DEx).

Security Classification:

Sensitive But Unclassified.

System Location:

Records will be located at the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division, 1000 Custer Hollow Road, Clarksburg, WV 26306, appropriate locations for system back-up and continuity of operations purposes.

Categories of Individuals Covered by the System:

The N-DEx will cover any individual who is identified in a law enforcement report concerning a crime incident or criminal investigation. These individuals include, but are not limited to: Subjects; suspects; associates; victims; persons of interest; witnesses; and/or any individual named in an arrest, booking, parole and/or probation report.

Categories of Records in the System:

The N-DEx will contain information collected by criminal justice agencies that is needed for the performance of their legally authorized, required function. The records in the system consist of incident, offense and case reports as well as arrest, booking, incarceration, and parole and probation information from Federal, State, local and tribal law enforcement entities. Other information in this system will include, but not be limited to: Name(s); sex; race; citizenship; date and place of birth; address(es); telephone number(s); social security number(s) or unique identifiers; physical description (including height, weight, hair color, eye color, gender, occupation and vehicle identifiers. Data from the FBI's CJIS Division, including the National Crime Information Center (NCIC), the Interstate Identification Index (III), and Integrated Automated Fingerprint Identification System (IAFIS), will be made available to the system queries, but the N-DEx will not contain copies of these databases. The information contributed by Federal, State, local and tribal law enforcement entities will be formatted using the National Information Exchange Model (NIEM), a single standard Extensible Markup Language (XML) foundation for exchanging information between agencies, in order to facilitate information sharing.

Authority for Maintenance of the System:

The system is established and maintained in accordance with 28 U.S.C. 533, 534; 28 C and 28 CFR part 20.

Purpose(s):

The purpose of the N-DEx system is to enhance the interconnectivity of criminal justice databases in order to improve the sharing of multiple levels of criminal justice data to further criminal justice objectives for crime analysis, law enforcement administration, and strategic/tactical operations in investigating, reporting, solving, and preventing crime, and thereby, improving homeland security. The N-DEx system will allow Federal, State, local, and tribal law enforcement agencies to compare and/or link criminal incidents and/or investigations occurring in their own jurisdictions with those in other jurisdictions throughout the country.

Routine Uses of Records Maintained in the System, Including categories of Users and Purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to the FBI as a routine use pursuant to 5 U.S.C. 552a(b)(3), to the extent such disclosures are compatible with the purpose for which the information was collected, in accordance with the blanket routine uses established for FBI record systems. For current blanket routine uses, see Blanket Routine Uses (BRU) Applicable to More Than One FBI Privacy Act System of Records, Department of Justice/FBI-BRU, published in the *Federal Register* at 66 FR 33558 (June 22, 2001) and amended at 70 FR 7513 (Feb. 14, 2005). Routine uses are not meant to be mutually exclusive and may overlap in some cases. In addition, the FBI may disclose relevant system records as follows:

- A. To any criminal, civil, or regulatory law enforcement authority (whether Federal, State, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement or homeland security responsibilities.
- B. To a Federal, State, local, joint, tribal, foreign, international, or other public agency/organization, or to any person or entity in either the public or private sector, domestic or foreign, where such disclosure may facilitate the apprehension of fugitives, the location

missing persons, the location and/or return of stolen property or similar criminal justice objectives.

C. To any person or entity in either the public or private sector, domestic or foreign, if disclosure by the FBI to be reasonably necessary to elicit information or cooperation from the recipient use in furthering the purposes of the system.

D. To appropriate agencies, entities, and persons when (1) The Department of Justice suspects or has confirmed that the security or confidentiality of information in the system records has been compromised; (2) the Department of Justice has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or proper interests, identity theft, or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department of Justice efforts to respond to the suspected or confirmed compromise and prevent, minimize, or eliminate such harm.

E. To those agencies, entities and persons the FBI may consider necessary or appropriate in the event of an incident to the ensuring the continuity of government functions in the event of any actual or potential significant disruption of normal operations.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Not Applicable.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Most information is maintained in electronic form and stored in computer memory, on disk storage, on computer tape, or other computer media. However, some information may also be maintained by the contributing agency in hard copy (paper) or other form.

RETRIEVABILITY:

Information will be retrieved by linkages based on identifying data collected on involved persons, places and things, and other non-specific descriptions of circumstances to identify events with a common modus operandi. This could include individual names or other personal identifiers.

SAFEGUARDS:

System records are maintained in limited access space in FBI controlled facilities and on computerized data is password protected. All FBI personnel are required to pass an external background investigation. The information is accessed only by authorized DOJ personnel or non-DOJ personnel properly authorized to assist in the conduct of an agency function related to these records. Authorized system users will have adequate physical security and built-in controls to protect against unauthorized personnel gaining access to the equipment and information stored in it.

RETENTION AND DISPOSAL:

The information within the N-DEX system will be contributed by Federal, State, local, and law enforcement entities. All entities will be responsible for ensuring the relevance and currency of the information they contribute to the system and will have control and responsibility for the disposition of their own records through a process that will be documented by a memorandum of understanding or based upon Federal law. Those portions of the N-DEX that constitute Federal records will be subject to retention schedules for those documents that have been approved by the National Archives and Records Administration (NARA). In addition, N-DEX, itself, will result in the creation of metadata or an audit trail that reflects any correlation between any of the submitted records, as well as information on user activity. A schedule for disposition of this metadata will be submitted to NARA for approval.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Federal Bureau of Investigation, 935 Pennsylvania Ave., NW., Washington, DC 20535-0001.

NOTIFICATION PROCEDURES:

Same as Record Access Procedures.

RECORD ACCESS PROCEDURES:

Because this system contains law enforcement records, the records in this system have been exempted from notification, access, and amendment to the extent permitted by subsection (b) of the Privacy Act. An individual who is the subject of one or more records in this system will be notified of records that are not exempt from notification and, accordingly, may access those records that are not exempt from disclosure. A request for access to a non-exempt record must be made in writing with the envelope and the letter clearly marked "Privacy Act Request." Requests should include full name and complete address and be signed. To verify the signature it must be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. Other identifying data that will assist in making a proper search of the system may also be submitted. Requests for access must be addressed to the Record/Information Dissemination Section, Federal Bureau of Investigation, 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001.

A determination on notification and access, in the sole prerogative of the FBI, will be made at the time a request is received.

CONTESTING RECORD PROCEDURES:

To contest or amend information maintained in the system, an individual should direct his or her request to the address provided above, stating clearly and concisely what information is contested, the reasons for contesting it, and the proposed amendment to the information sought.

Some information may be exempt from contesting record procedures as described in the section titled "Exemptions Claimed for the System." An individual who is the subject of one or more records in this system may contest and pursue amendment of those records that are not exempt. A determination whether a record may be subject to amendment will be made at the time a request is received.

RECORD SOURCE CATEGORIES:

Information contained in the N-DEx system is obtained from Federal, State, local, and tribal law enforcement agencies.

criminal justice agencies.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system from subsection (c)(3) and (4); (d)(1), (4) and (5); (e)(1), (2), (3), (5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (e), and are published in today's *Federal Register*.

[\[TOP\]](#)

JUSTICE/FBI-999

System name: Appendix of Field Divisions for the Federal Bureau of Investigation.

Field Office:

502 U.S. Post Office & Court House

Albany, New York 12207

4303 Federal Office Building

Albuquerque, New Mexico 87101

Room 500, 300 North Lee Street

Alexandria, Virginia 22314

Room 238, Federal Building

Anchorage, Alaska 99510

275 Peachtree Street, NE

Atlanta, Georgia 30303

7142 Ambassador Road

Baltimore, Maryland 21207

Room 1400 - 2121 Building

Birmingham, Alabama 35203

John F. Kennedy Federal Office Building

Boston, Massachusetts 02203

Room 1400 - 111 West Huron Street

Buffalo, New York 14202

115 U.S. Court House and Federal Building

Butte, Montana 59701

1120 Jefferson Standard Life Building

Charlotte, North Carolina 28202

Room 905, Everett McKinley Dirksen Building

Chicago, Illinois 60604

415 U.S. Post Office & Court House Building

Cincinnati, Ohio 45202

3005 Federal Office Building

Cleveland, Ohio 44199

1529 Hampton Street

Columbia, South Carolina 29201

Room 200, 1810 Commerce Street

Dallas, Texas 75201

Room 18218, Federal Office Building

Denver, Colorado 80202

Patrick V. McNamara Building

477 Michigan Avenue

Detroit, Michigan 48226

202 U.S. Court House Building

El Paso, Texas 79901

Kalanianaʻole Federal Building

Room 4307

300 Ala Moana Boulevard

Honolulu, Hawaii 96850

6015 Federal Building and U.S. Court House

Houston, Texas 77002

575 North Pennsylvania St.

Indianapolis, Indiana 46202

800 Unifirst Federal Savings & Loan Building

Jackson, Mississippi 39205

414 U.S. Court House & Post Office Building

Jacksonville, Florida 32202

Room 300 - U.S. Courthouse

Kansas City, Missouri 64106

Room 800, 1111 Northshore Drive

Knoxville, Tennessee 37919

Room 2-011, Federal Office Building

Las Vegas, Nevada 89101

215 U.S. Post Office Building

Little Rock, Arkansas 72201

11000 Wilshire Boulevard

Los Angeles, California 90024

Room 502, Federal Building

Louisville, Kentucky 40202

841 Clifford Davis Federal Building

Memphis, Tennessee 38103

3801 Biscayne Boulevard

Miami, Florida 33137

Room 700, Federal Building and U.S. Court House

Milwaukee, Wisconsin 53202

392 Federal Building

Minneapolis, Minnesota 55401

520 Federal Building

Mobile, Alabama 36602

Gateway I, Market Street

Newark, New Jersey 07101

770 Chapel Building

New Haven, Connecticut 06510

701 Loyola Avenue

New Orleans, Louisiana 70113

201 East 69th Street

New York, New York 10021

Room 300, 870 Military Highway

Norfolk, Virginia 23502

50 Penn Place, N.W., 50th at Pennsylvania

Oklahoma City, Oklahoma 73118

1010 Federal Office Building

Omaha, Nebraska 68102

8th Floor, Federal Office Building

600 Arch Street

Philadelphia, Pennsylvania 19106

2721 North Central Avenue

Phoenix, Arizona 85004

1300 Federal Office Building

Pittsburgh, Pennsylvania 15222

Crown Plaza Building

Portland, Oregon 97201

200 West Grace Street

Richmond, Virginia 23220

Federal Building

2800 Cottage Way

Sacramento, California 95825

2704 Federal Building

St. Louis, Missouri 63103

3203 Federal Building

Salt Lake City, Utah 84138

433 Federal Building

Box 1630

San Antonio, Texas 78296

Federal Office Building

Room 6531

88 Front Street

San Diego, California 92188

450 Golden Gate Avenue

San Francisco, California 94102

U.S. Courthouse and Federal Building

Room 526

Hato Rey, Puerto Rico 00918

5401 Paulsen Street

Savannah, Georgia 31405

915 Second Avenue

Seattle, Washington 98174

535 West Jefferson Street

Springfield, Illinois 62702

Room 610, Federal Office Building

Tampa, Florida 33602

506 Old Post Office Building

Washington, DC 20535

Federal Bureau of Investigation Academy

Quantico, Virginia 22135

LEGAL ATTACHE (all c/o The American Embassy for the cities indicated):

Bern, Switzerland

Bonn, Germany (Box 310, APO, New York 09080)

Buenos Aires, Argentina

Caracas, Venezuela (APO, New York 09893)

Hong Kong, B.C.C. (FPO, San Francisco 96659)

London, England (Box 40, FPO, New York 09510)

Madrid, Spain (APO, New York 09285)

Manila, Philippines (APO, San Francisco 96528)

Mexico City, Mexico

Ottawa, Canada

Paris, France (APO, New York 09777)

Rome, Italy (APO, New York 09794)

Tokyo, Japan (APO, San Francisco 96503)

[\[TOP\]](#)

Foreign Claims Settlement Commission

JUSTICE/FCSC-1

System name:

Indexes of Claimants (Alphabetical)—FCSC.

System location:

Foreign Claims Settlement Commission, 600 E Street, Northwest, Suite 6002, Washington, D.C. 20579.

Categories of individuals covered by the system:

Maintained on all individuals who filed claims for compensation under the statutes administered by the Foreign Claims Settlement Commission.

Categories of records in the system:

Microfilm copies of index cards and computer-generated paper indexes containing names of claimants, claim and decision numbers, date and disposition of claims, addresses and date of birth.

Authority for maintenance of the system:

5 U.S.C. 301.

Purpose(s):

To enable Commission personnel and interested members of the public to ascertain whether any named individual, corporation, or other legal entity has submitted a claim to the Commission.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Used by authorized Commission personnel for identification of individual claims and the information concerning disposition of claims.

—The information contained in this system of records (except for that pertaining to the system "Justice/FCSC-27: Germany, Holocaust Survivors Claims Against" , described below) is considered by the Commission to be public information which may be disclosed as a routine use to interested persons who make inquiries about the claims program or individual claims therein, including but not limited to Members of Congress or congressional staff, staff of the Office of Management and Budget, other persons interested in the work of the Commission, and members of the news media.

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as set forth in OMB Circular No. A-19, at any stage of the legislative coordination and clearance process as set forth in that circular.

—A record from this system of records may be disclosed as a routine use to a Member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the request of the individual about whom the record is maintained.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof,
- ii. Any employee of the FCSC in his or her official capacity,

iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or

iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Microfilm rolls stored in steel drawers. Computer-generated paper indexes stored on shelf and cardboard binders.

Retrievability:

By name of individual.

Safeguards:

Security guards in building. Records maintained in locked rooms accessible only to authorized Federal Claims Commission personnel.

Retention and disposal:

Permanent records. Disposition will be made in accordance with 44 U.S.C. 3301–3314 and such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616–6986 Fax: 202/616–6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Individual on whom the record is maintained and information obtained by actions taken Foreign Claims Settlement Commission as a result of adjudication of individual claims.

[\[TOP\]](#)

JUSTICE/FCSC-3

System name:

Certification of Awards—FCSC.

System location:

Foreign Claims Settlement Commission, 600 E Street, Northwest, Suite 6002, Washington 20579.

Categories of Individuals covered by the system:

Individuals receiving awards under the International Claims Settlement Act of 1949, as amended, and War Claims Act of 1948, as amended.

Categories of records in the system:

Names and addresses of claimants and amounts of awards certified to Treasury Department for payment. Name and address of claimant's representative, if any, also included in certification voucher.

Authority for maintenance of the system:

International Claims Settlement Act of 1949, as amended, and War Claims Act of 1948, amended.

Purpose(s):

Maintained as a record of the names, addresses, and amounts awarded to individuals in Commission's claims programs.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee if such communication may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Award certifications prepared by authorized FCSC personnel and forwarded to Treasury Department for payment in accordance with statutory authority and Treasury Department regulations and procedures.

—The information contained in this system of records (except for that pertaining to the subject "Justice/FCSC-27: Germany, Holocaust Survivors Claims Against") is considered by the Commission to be public information which may be disclosed as a routine use to interest

persons who make inquiries about a claims program or individual claims therein, including not limited to Members of Congress or congressional staff, staff of the Office of Management and Budget, other persons interested in the work of the Commission, and members of the news media.

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as set forth in OMB Circular No. A–19, at any stage of the legislative coordination and clearance process as set forth in that circular.

—A record from this system of records may be disclosed as a routine use to a member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the request of the individual about whom the record is maintained.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her individual capacity where

the Department of Justice has agreed to represent the employee, or

- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Contained in file folders.

Retrievability:

By voucher number and date of certification.

Safeguards:

Building has building guards. Records are maintained in file cabinets in locked rooms.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance with 44 U.S.C. 3301–3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616–6975. Fax: 202/616–6993. Notification Procedure: Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

From award portion of decisions as determined by FCSC.

[\[TOP\]](#)

JUSTICE/FCSC–4

System name:

China, Claims Against—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

U.S. nationals with claims for property losses, death and disability in mainland China and Hong Kong between October 1, 1949, and May 11, 1979.

Categories of records in the system:

Claim application form containing name and address of claimant and representative, if any; date and place of birth or naturalization of claimant; nature and amount of claim; description of property; ownership and value of property; and evidence to support claim.

Authority for maintenance of the system:

Titles I and V, International Claims Settlement Act of 1949, as amended, and the U.S.-China Claims Settlement Agreement of May 11, 1979.

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the valid amount of the claims submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity, fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee if such communication may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Adjudication of claims, issuance of decisions as to the validity and amounts of claims and issuance of certifications to each individual claimant as to amount determined by FCSC and personnel. Such amounts and copies of FCSC decisions were certified to the Secretary of State and to the Secretary of the Treasury.

—The information contained in this system of records is considered by the Commission to be public information which may be disclosed as a routine use to interested persons who make inquiries about the claims program or individual claims therein, including but not limited to Members of Congress or congressional staff, staff of the Office of Management and Budget, and other persons interested in the work of the Commission, and members of the news media.

—Law enforcement: In the event that a system of records maintained by FCSC to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute, particular program statute, or by regulatory rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as set forth in OMB Circular No. A-19, at any stage of the legislative coordination and clearance process as set forth in that circular.

—A record from this system of records may be disclosed as a routine use to a member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the request of the individual about whom the record is maintained.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by claim number. File folders retrieved from Records Center by claim number. Alphabetical index used for identification of claim (see system "Justice/FCSC—Records" above).

Safeguards:

Under security safeguards at Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance with 5 U.S.C. 301.

44 U.S.C. 3301–3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616–6975, Fax: 202/616–6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Individual on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC–5

System name:

Civilian Internees (Vietnam)—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

American citizens held by a hostile force in Southeast Asia during Vietnam Conflict.

Categories of records in the system:

Claim application form contains name and address, date and place of birth, birth certifi

Verification of internment furnished by State Department contains names, addresses and inclusive dates of internment.

Authority for maintenance of the system:

Section 5(i), War Claims Act of 1948, as amended.

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the valid amount of the claims submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee if such communication may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Adjudication of claims of American citizens and certification of awards by authorized Federal personnel to Treasury Department for payment.

—The information contained in this system of records is considered by the Commission

public information which may be disclosed as a routine use to interested persons who make inquiries about the claims program or individual claims therein, including but not limited to Members of Congress or congressional staff, staff of the Office of Management and Budget, and other persons interested in the work of the Commission, and members of the news media.

—Law enforcement: In the event that a system of records maintained by FCSC to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether federal, state, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as set forth in OMB Circular No. A-19, at any stage of the legislative coordination and clearance process as set forth in that circular.

—A record from this system of records may be disclosed as a routine use to a member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the request of the individual about whom the record is maintained.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is in the public interest.

disclosure is determined by the FCSC to be a use compatible with the purpose for which records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed by claim number. (see system "Justice/FCSC-1" above).

Safeguards:

Under security safeguards at Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance with 44 U.S.C. 3301-3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616-6975. Fax: 202/616-6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Individual on whom record is maintained, or his or her survivor(s), where applicable.

[\[TOP\]](#)

JUSTICE/FCSC-8

System name:

Cuba, Claims Against—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

U.S. nationals with claims for property losses, death and disability in Cuba arising on or January 1, 1959.

Categories of records in the system:

Claim application form containing name and address of claimant and representative, if any; date and place of birth or naturalization; nature and amount of claim; description, ownership and value of property; and evidence to support claim, including medical and death records; claims involving death and disability.

Authority for maintenance of the system:

Title V, International Claims Settlement Act of 1949, as amended.

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the valid amount of the claims against Cuba submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee if such disclosure may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Adjudication of claims, issuance of decisions as to the validity and amounts of claims and issuance of certifications to each individual claimant as to amount determined by FCSC and personnel. Such amounts and copies of FCSC decisions were certified to the Secretary of State pending conclusion of any claims settlement agreement between US and Cuba.

—The information contained in this system of records is considered by the Commission to be public information which may be disclosed as a routine use to interested persons who make inquiries about the claims program or individual claims therein, including but not limited to Members of Congress or congressional staff, staff of the Office of Management and Budget, and other persons interested in the work of the Commission, and members of the news media.

—Law enforcement: In the event that a system of records maintained by FCSC to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as set forth in OMB Circular No. A–19, at any stage of the legislative coordination and clearance process as set forth in that circular.

—A record from this system of records may be disclosed as a routine use to a member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the request of the individual about whom the record is maintained.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by claim number. File Folders retrieved from Records Center by claim

number. Alphabetical index used for identification of claim (see system "Justice/FCSC—above).

Safeguards:

Under security safeguards at Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance 44 U.S.C. 3301–3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616–6975. Fax: 202/616–6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Individual on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC–9

System name:

Czechoslovakia, Claims Against (2nd Program)—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

U.S. nationals with claims for property losses in Czechoslovakia from August 9, 1958, to February 2, 1982.

Categories of records in the system:

Claim application form containing name and address of claimant and representative, if any; date and place of birth or naturalization; nature and amount of claim; description, ownership, and value of property; and evidence to support claim for the purpose of receiving compensation.

Authority for maintenance of the system:

Czechoslovakian Claims Settlement Act of 1981 (22 U.S.C. note prec. 1642), and the U.S.-Czechoslovakian Claims Settlement Agreement of February 2, 1982.

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the valid amount of the claims against Czechoslovakia submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee if such communication may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Records were used for the purpose of adjudicating claims of individuals; issuance of decisions concerning eligibility to receive compensation under the Act; notifications to claimants of rights to appeal; and preparation by authorized FCSC personnel of certifications of awards to the Treasury Department for payment. Names and other data furnished by claimants were used for verifying citizenship status with INS.

—The information contained in this system of records is considered by the Commission to be public information which may be disclosed as a routine use to interested persons who make inquiries about the claims program or individual claims therein, including but not limited to Members of Congress or congressional staff, staff of the Office of Management and Budget, and other persons interested in the work of the Commission, and members of the news media.

—Law enforcement: In the event that a system of records maintained by FCSC to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as set forth in OMB Circular No. A-19, at any stage of the legislative coordination and clearance process as set forth in that circular.

—A record from this system of records may be disclosed as a routine use to a member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the request of the individual about whom the record is maintained.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by claim number. File folders retrieved from Records Center by claim number. Alphabetical index used for identification of claim (see system "Justice/FCSC—Records" above).

Safeguards:

Under security safeguards at Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance with 5 U.S.C. 301.

44 U.S.C. 3301–3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616–6975. Fax: 202/616–6993.

Notification procedure:

Set forth in part 504 of Title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Individual on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC–10

System name:

East Germany, Registration of Claims Against—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

U.S. nationals who suffered certain property losses in East Germany.

Categories of records in the system:

Claims registration form containing name and address of claimant and representative, if

date and place of birth or naturalization; nature and amount of claim; and description, ownership, and value of property.

Authority for maintenance of the system:

Title I, International Claims Settlement Act of 1949, as amended.

Purpose(s):

To enable the Commission to conduct an evaluation of potential claims against the former German Democratic Republic, in order to determine whether sufficient claims existed to warrant enactment of legislation authorizing a formal claims adjudication program.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee of the Commission where the disclosure may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Information received from individuals on registration forms was used to evaluate whether to propose enactment of legislation to authorize a formal claims adjudication program.

—Registration forms filed were also used by FCSC personnel in the distribution of form application forms once a formal claims adjudication program was authorized.

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as set forth in OMB Circular No. A-19, at any stage of the legislative coordination and clearance process as set forth in that circular.

—A record from this system of records may be disclosed as a routine use to a member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the request of the individual about whom the record is maintained.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Numerical order in file folders. Cross-reference alphabetical index (see system "JUSTICE/FCSC-1" above).

Retrievability:

By name. (see system "JUSTICE/FCSC-1" above).

Safeguards:

Under security safeguards at Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance with 44 U.S.C. 3301-3314 when such records are determined no longer useful. System manager and address: Administrative Office, Foreign Claims Settlement Commission, 600 E Street Northwest, Suite 6002, Washington, DC 20579. Telephone: 202/616-6975. Fax: 202/616-6976.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Individual on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC-11***System name:***

Federal Republic of Germany, Questionnaire Inquiries From—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

Individuals suffering losses in Eastern European countries, including Germany.

Categories of records in the system:

Questionnaires from Federal Republic of Germany (Ausgleichsamt) containing name, a date and place of birth or naturalization; description and location of property. Such information was furnished to Federal Republic of Germany by U.S. residents who filed claims under West German Federal Compensation Laws (BEG).

Authority for maintenance of the system:

5 U.S.C. 301.

Purpose(s):

To maintain a file on requests for information from Germany that have been received and responded upon.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee

Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding matter within that person's former area of responsibility.

—To inform Federal Republic Of Germany (FRG) Equalization of Burdens offices whether individuals who filed claims for losses compensable under the West German Federal Compensation Laws also filed claims with the Foreign Claims Settlement Commission under U.S. claims statutes and received compensation under such statutes for the same losses. Information furnished to FRG obtained from FCSC decisions or claim applications from individuals who filed claims with FCSC.

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as set forth in OMB Circular No. A-19, at any stage of the legislative coordination and clearance process as set forth in that circular.

—A record from this system of records may be disclosed as a routine use to a member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the request of the individual about whom the record is maintained.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records

determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Paper records in file folders.

Retrievability:

By name.

Safeguards:

Under security safeguards at Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance with 44 U.S.C. 3301–3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616–6975.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Questionnaire from Federal Republic of Germany (Equalization of Burdens Offices).

[\[TOP\]](#)

JUSTICE/FCSC-12

System name:

Hungary, Claims Against (2nd Program)—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

U.S. nationals with claims for property losses in Hungary that arose between August 9, 1945, and March 6, 1973.

Categories of records in the system:

Claim application form containing name and address of claimant and representative, if any; date and place of birth or naturalization; nature and amount of claim; description, ownership, and value of property; and evidence to support claim for the purpose of receiving compensation.

Authority for maintenance of the system:

Title III, International Claims Settlement Act of 1949, as amended, and U.S.-Hungarian Claims Agreement of March 6, 1973.

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the valid amount of the claims against Hungary submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Records were used for the purpose of adjudicating claims of individuals; issuance of decisions concerning eligibility to receive compensation under the Act; notifications to claimants of rights to appeal; and preparation by authorized FCSC personnel of certifications of awards, if any, to Treasury Department for payment. Names and other data furnished by claimants were used for verifying citizenship status with INS.

—The information contained in this system of records is considered by the Commission to be public information which may be disclosed as a routine use to interested persons who make inquiries about the claims program or individual claims therein, including but not limited to Members of Congress or congressional staff, staff of the Office of Management and Budget, and other persons interested in the work of the Commission, and members of the news media.

—Law enforcement: In the event that a system of records maintained by FCSC to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation.

rule or order issued pursuant thereto, the relevant records in the system of records may referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged enforcing or implementing the statute, or rule, regulation or order issued pursuant there

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as set forth in OMB Circular No. A-19, at any stage of the legislative coordination and clearance process as set forth in that circular.

—A record from this system of records may be disclosed as a routine use to a member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the request of the individual about whom the record is maintained.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by claim number. Alphabetical index used for identification of claim (system "Justice/FCSC-1" above).

Safeguards:

Under security safeguards at Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance with 44 U.S.C. 3301-3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616-6975. Fax: 202/616-6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Individual on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC-14

System name:

Micronesia, Claims Arising In—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

Inhabitants of Micronesia, including U.S. nationals, who suffered damages to property, disability and death arising out of military operations during World War II, and arising during the period from the dates of the securing of the various islands of Micronesia by Allied forces up until July 1, 1951.

Categories of records in the system:

Claim application forms containing name and address of claimant and representative, if date and place of birth or naturalization; nature and amount of claim; description, ownership and value of property; and evidence to support claim for the purpose of receiving compensation.

Authority for maintenance of the system:

Micronesian Claims Act of 1971.

Purpose(s):

To enable the Micronesian Claims Commission (MCC), under the supervision of the FCSC, to carry out its statutory responsibility to determine the validity and amount of the claims and Italy submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity

fraud, or harm to the security or integrity of this system or other systems or programs (w maintained by the Commission or another agency or entity) that rely upon the comprom information; and (3) the disclosure made to such agencies, entities, and persons is reas necessary to assist in connection with the Commission's efforts to respond to the suspe confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee Commission for purposes of: responding to an official inquiry by a federal, state, or loca government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employe may be necessary for personnel-related or other official purposes where the Commissio requires information and/or consultation assistance from the former employee regarding matter within that person's former area of responsibility.

—Records were used for the purpose of adjudicating claims of individuals; issuance of decisions concerning eligibility to receive compensation under authority of the Micronesi Claims Act of 1971; notifications to claimants of rights to appeal; and preparation by aut personnel of Foreign Claims Settlement Commission assigned to duty in the Trust Terri the Pacific Islands and locally hired employees of the MCC of certifications of awards, if Secretary of the Interior for payment.

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as se in OMB Circular No. A-19, at any stage of the legislative coordination and clearance pro as set forth in that circular.

—A record from this system of records may be disclosed as a routine use to a member Congress or to a congressional staff member in response to an inquiry of the congressi office made at the request of the individual about whom the record is maintained.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a c adjudicative body before which the FCSC is authorized to appear or to the Department Justice for use in such proceeding when:

i. The FCSC, or any subdivision thereof, or

- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by claim number. Alphabetical index used to identify claim (see system "Justice/FCSC-1" above).

Safeguards:

Under security safeguards at Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance with 44 U.S.C. 3301–3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616–6975. Fax: 202/616–6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Individual on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC-16

System name:

Prisoners of War (Pueblo)—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

Members of the U.S. Armed Forces and civilian employees of the U.S. Government assigned duty on the USS Pueblo who were captured by military forces of North Korea on January 31, 1968, and held prisoner by such forces.

Categories of records in the system:

Claim application form containing name and address of claimant, date and places of birth, branch of service and military service number. In case of death, date, place and name of spouse, names, address and date of birth of surviving children, name and address of parents and Veterans Administration (VA) claim number. Proof of death if no VA claim.

Authority for maintenance of the system:

Section 6(e), War Claims Act of 1948, as amended.

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the valid amount of the claims submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee of the Commission may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Records were used for adjudication of claims for detention benefits, issuance of decisions concerning eligibility of claimant to receive compensation; notifications to claimants of right of appeal; and preparation by authorized Commission personnel of certifications of awards to the Treasury Department for payment. Verifications from State Department include names and addresses and inclusive dates of detention.

—The information contained in this system of records is considered by the Commission

public information which may be disclosed as a routine use to interested persons who make inquiries about the claims program or individual claims therein, including but not limited to Members of Congress or congressional staff, staff of the Office of Management and Budget, and other persons interested in the work of the Commission, and members of the news media.

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as set forth in OMB Circular No. A-19, at any stage of the legislative coordination and clearance process as set forth in that circular.

—A record from this system of records may be disclosed as a routine use to a member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the request of the individual about whom the record is maintained.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records in file folders.

Retrievability:

By claim number. Cross-referenced by alphabetical index cards which contain claim number (see system "Justice/FCSC-1" above).

Safeguards:

Under security safeguards at the Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance with 44 U.S.C. 3301-3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616-6975. Fax: 202/616-6993.

Notification procedure:

Set forth in part 504 of Title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Individual on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC-17

System name:

Prisoners of War (Vietnam)—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

Members of Armed Forces of the United States who were captured and held by a hostile power during the Vietnam conflict beginning February 28, 1961.

Categories of records in the system:

Claim application form containing name and address of claimant; date and place of birth; branch of service and military service number. In case of death, date, place, name of spouse, names, addresses and dates of birth of surviving children, name and address of parent; Veterans Administration claim number.

Authority for maintenance of the system:

Sect. 6(f), War Claims Act of 1948, as amended.

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the valid amount of the claims submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonable.

necessary to assist in connection with the Commission's efforts to respond to the suspected compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Records used for adjudication of claims for detention benefits; issuance of decisions concerning eligibility of claimants to receive compensation; notifications to claimants of an appeal; and preparation of certification of awards to Treasury Department for payment to authorized Commission personnel. Verification of captured status obtained from rosters and casualty reports furnished by the respective armed service branches.

—The information contained in this system of records is considered by the Commission to be public information which may be disclosed as a routine use to interested persons who make inquiries about the claims program or individual claims therein, including but not limited to Members of Congress or congressional staff, staff of the Office of Management and Budget, and other persons interested in the work of the Commission, and members of the news media.

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as set forth in OMB Circular No. A-19, at any stage of the legislative coordination and clearance process as set forth in that circular.

—A record from this system of records may be disclosed as a routine use to a member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the request of the individual about whom the record is maintained.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by claim number. File folders retrieved from Records Center by claim number. Alphabetical index used for identification of claim (see system "Justice/FCSC—Records" above).

Safeguards:

Under security safeguards at Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance with 44 U.S.C. 3301–3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616-6975. Fax: 202/616-6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Individual on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC-19

System name:

Soviet Union, Claims Against—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

U.S. nationals with claims for loss of property in the Soviet Union prior to November 16, and claims by individuals based upon liens acquired with respect to property in the U.S assigned to U.S. Government by the Soviet Government under Litvinov Assignment of November 16, 1933.

Categories of records in the system:

Claim application form containing name and address of claimant and representative, if a

date and place of birth or naturalization; nature and amount of claim; description, owner, and value of property; and evidence to support claim for the purpose of receiving compensation.

Authority for maintenance of the system:

Title III, International Claims Settlement Act of 1949, as amended.

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the valid amount of the claims against the Soviet Union submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee of the Commission may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Records were used for the purpose of adjudicating claims of individuals; issuance of decisions concerning eligibility to receive compensation under the Act; notifications to claimants of rights to appeal; and preparation by authorized FCSC personnel of certifications of a

if any, to the Treasury Department for payment. Names and other data furnished by claimant used for verifying citizenship status with INS.

—The information contained in this system of records is considered by the Commission to be public information which may be disclosed as a routine use to interested persons who make inquiries about the claims program or individual claims therein, including but not limited to Members of Congress or congressional staff, staff of the Office of Management and Budget, and other persons interested in the work of the Commission, and members of the news media.

—Law enforcement: In the event that a system of records maintained by FCSC to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulatory rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as set forth in OMB Circular No. A-19, at any stage of the legislative coordination and clearance process as set forth in that circular.

—A record from this system of records may be disclosed as a routine use to a member of Congress or to a congressional staff member in response to an inquiry of the congressional office made at the request of the individual about whom the record is maintained.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or

iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by claim number. File folders retrieved from Records Center by claim number. Alphabetical index used for identification of claim (see system "Justice/FCSC—Records" above).

Safeguards:

Under security safeguards at Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance with 44 U.S.C. 3301–3314 when such records are determined no longer useful. This system of records was retired to the Washington National Records Center after the completion of the claims program on August 9, 1959.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616–6975. Fax: 202/616–6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Individual on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC-21

System name:

German Democratic Republic, Claims Against—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

U.S. nationals with claims for property losses in the German Democratic Republic which between May 8, 1945, and October 18, 1976.

Categories of records in the system:

Claim application form containing name and address of claimant and representative, if any; date and place of birth or naturalization; nature and amount of claim; description, ownership, and value of property; and evidence to support claim for the purpose of receiving compensation.

Authority for maintenance of the system:

Title VI, International Claims Settlement Act of 1949, as amended.

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the valid amount of the claims against the German Democratic Republic submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee of the Commission may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Records were used for the purpose of adjudicating claims of individuals; issuance of decisions concerning eligibility to receive compensation under the Act; notification to claimants of rights to appeal; and preparation of certifications of awards, if any, to Treasury Department for payment. Names and other data furnished by claimants used for verifying citizenship with INS.

—The information contained in this system of records is considered by the Commission to be public information which may be disclosed as a routine use to interested persons who make inquiries about the claims program or individual claims therein, including but not limited to Members of Congress or congressional staff, staff of the Office of Management and Budget,

other persons interested in the work of the Commission, and members of the news media.

—Law Enforcement: In the event that a system of records maintained by FCSC to carry out its functions indicates a violation or potential violation of law, whether civil or criminal or regulatory in nature, and whether arising by general statute or particular program statute or order issued pursuant thereto, the relevant records in the system of records may be referred, as a reference, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto.

—The information contained in this system of records will be disclosed to the Office of Management and Budget in connection with the review of private relief legislation as set forth in OMB Circular No. A-19, at any stage of the legislative coordination and clearance process set forth in that circular.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect any of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the FCSC to be arguably relevant and necessary to the litigation and disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by claim number. Alphabetical index used for identification of claim (system "Justice/FCSC-1" above).

Safeguards:

Under security safeguards at Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal in accordance with 44 U.S.C. 3301-3 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616-6975. Fax: 202/616-6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Claimant on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC-23

System name:

Vietnam, Claims for Losses Against—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

U.S. nationals with claims for property losses in Vietnam arising between April 29, 1975 and December 28, 1980.

Categories of records in the system:

Claim application forms containing name and address of claimant and representative, if date and place of birth or naturalization; nature and amount of claim; description, owner, and value of property; and evidence to support claim for the purpose of receiving compensation.

Authority for maintenance of the system:

Title VII, International Claims Settlement Act of 1949, as amended.

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the valid amount of the claims against Vietnam submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (w

maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonable and necessary to assist in connection with the Commission's efforts to respond to the suspected compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Records were used for the purpose of adjudicating claims of individuals; issuance of decisions concerning eligibility to receive compensation under the Act; notifications to claimants of rights to appeal; and preparation of certifications of awards, if any, to Treasury Department for payment. Names and other data furnished by claimants used for verifying citizenship with INS.

—The information contained in this system of records is considered by the Commission to be public information which may be disclosed as a routine use to interested persons who make inquiries about the claims program or individual claims therein, including but not limited to members of Congress, Congressional staff, staff of the Office of Management and Budget, and other persons interested in the work of the Commission, and members of the news media.

—Law Enforcement: In the event that a system of records maintained by FCSC to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether federal, state, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

—The information contained in this system of records will be disclosed to the Office of Management and Budget, in connection with the review of private relief legislation as set forth in OMB Circular No. A-19, at any stage of the legislative coordination and clearance process as set forth in that circular.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions is a party to litigation or has an interest in litigation and such records are determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by claim number. Alphabetical index used for identification of claim (see system "Justice/FCSC-1" above).

Safeguards:

Under security safeguards at Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance with

44 U.S.C. 3301–3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616–6975. Fax: 202/616–6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Individual on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC–24

System name:

Ethiopia, Claims for Losses Against—FCSC.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

U.S. nationals with claims for property losses in Ethiopia.

Categories of records in the system:

Claims information including name and address of claimant and representative, if any; c

and place of birth or naturalization; nature and amount of claim; description, ownership, value of property; and evidence to support claim for the purpose of receiving compensa

Authority for maintenance of the system:

Title I, International Claims Settlement Act of 1949, as amended, and the December 19, Compensation Agreement between the Government of the United States of America and Provisional Military Government of Socialist Ethiopia.

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the valid amount of the claims against Ethiopia submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (not maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonable necessary to assist in connection with the Commission's efforts to respond to the suspected confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee if necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Records are used for the purpose of adjudicating claims of individuals; issuance of decisions concerning eligibility to receive compensation under the Act; notifications to claimants of

to appeal; and preparation of certifications of awards, if any, to the Treasury Department payment. Names and other data furnished by claimants used for verifying citizenship status with INS.

—The information contained in this system of records is considered by the Commission public information which may be disclosed as a routine use to interested persons who make inquiries about the claims program or individual claims therein, including but not limited to members of Congress, Congressional staff, staff of the Office of Management and Budget, and other persons interested in the work of the Commission, and members of the news media.

—Law Enforcement: In the event that a system of records maintained by FCSC to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether federal, state, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity or
- iii. Any employee of the FCSC in his or her individual capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions is a party to litigation or has an interest in litigation and such records are determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by claim number. Alphabetical index used for identification of claim (system "Justice/FCSC-1" above).

Safeguards:

Under security safeguards at Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be made in accordance with 44 U.S.C. 3301–3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616–6975. Fax: 202/616–6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Claimant on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC-25

System name:

Egypt, Claims Against.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

U.S. nationals with claims for property losses in Egypt.

Categories of records in the system:

Claim information, including name and address of claimant and representative, if any; date of birth or naturalization; nature and amount of claim; description, ownership, and value of property; other evidence establishing entitlement to compensation of claim.

Authority for maintenance of the system:

Title I, International Claims Settlement Act of 1949, as amended, and the Agreement Between the Government of the United States of America and the Government of the Arab Republic of Egypt Concerning Claims of Nationals of the United States of May 1, 1976.

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the validity and amount of the claims against Egypt submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise, unauthorized persons may have gained access to information in the system of records; or (3) the Commission has determined that the information in the system of records is of such a nature that its unauthorized disclosure could result in the identification, location, or harm to an individual.

confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (w maintained by the Commission or another agency or entity) that rely upon the comprom information; and (3) the disclosure made to such agencies, entities, and persons is reas necessary to assist in connection with the Commission's efforts to respond to the suspe confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee Commission for purposes of: responding to an official inquiry by a federal, state, or loca government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employe may be necessary for personnel-related or other official purposes where the Commissio requires information and/or consultation assistance from the former employee regarding matter within that person's former area of responsibility.

—Records are used for the purpose of adjudicating claims of individuals; issuance of de concerning eligibility to receive compensation under the Act and Agreement; notification claimants of rights to appeal; and preparation of certifications of awards, if any, to the T Department for payment. Names and other information furnished by claimants may be u verifying citizenship status with the Immigration and Naturalization Service.

—The information contained in this system of records is considered by the Commission public information which may be disclosed as a routine use to interested persons who n inquiries about the claims program or individual claims therein including but not limited Members of Congress or Congressional staff, staff of the Office of Management and Bu other persons interested in the work of the Commission, and members of the news med

—Law Enforcement In the event that a system of records maintained by FCSC to carry functions indicates a violation or potential violation of law, whether civil or criminal or reg in nature and whether arising by general statute or particular program statute or order is pursuant thereto, the relevant records in the system of records may be referred, as a ro use, to the appropriate agency, whether Federal, State, local or foreign, charged with e or implementing the statute, or rule, regulation or order issued pursuant thereto.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a c adjudicative body before which the FCSC is authorized to appear or to the Department Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her official capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions is a party to litigation or has an interest in litigation and such records determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by claim number. Alphabetical index used for identification of claim (see system "Justice/FCSC'1" above).

Safeguards:

Under security safeguards at the Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be in accordance with 5 U.S.C. 3301–3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest,

6002, Washington, DC 20579. Telephone: 202/616-6975. Fax: 202/616-6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Claimant on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC-26

System name:

Albania, Claims Against.

System location:

Washington National Records Center, 4205 Suitland Road, Washington, DC 20409.

Categories of individuals covered by the system:

U.S. nationals with claims for property losses in Albania.

Categories of records in the system:

Claim information, including name and address of claimant and representative, if any; d place of birth or naturalization; nature and amount of claim; description, ownership, and of property; other evidence establishing entitlement to compensation of claim.

Authority for maintenance of the system:

Title I, International Claims Settlement Act of 1949, as amended, and the Agreement Between the Government of the United States of America and the Government of Albania on the Settlement of Certain Outstanding Claims of March 10, 1995 (went into force April 18, 1995).

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the valid amount of the claims against Albania submitted to it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee if such disclosure may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Records are used for the purpose of adjudicating claims of individuals; issuance of decisions concerning eligibility to receive compensation under the Act and Agreement; notification of claimants of rights to appeal; and preparation of certifications of awards, if any, to the Treasury Department for payment. Names and other information furnished by claimants may be used to verify citizenship status with the Immigration and Naturalization Service.

—The information contained in this system of records is considered by the Commission

public information which may be disclosed as a routine use to interested persons who make inquiries about the claims program or individual claims therein including but not limited to Members of Congress or Congressional staff, staff of the Office of Management and Budget, other persons interested in the work of the Commission, and members of the news media.

—Law Enforcement: In the event that a system of records maintained by FCSC to carry out its functions indicates a violation or potential violation of law, whether civil or criminal or regulatory in nature and whether arising by general statute or particular program statute or order is pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her official capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions is a party to litigation or has an interest in litigation and such records are determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by claim number. Alphabetical index used for identification of claim (system "Justice/FCSC-1" above).

Safeguards:

Under security safeguards at the Washington National Records Center.

Retention and disposal:

Records maintained under 5 U.S.C. 301. Disposal of records will be in accordance with U.S.C. 3301-3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, Northwest, 6002, Washington, DC 20579. Telephone: 202/616-6975. Fax: 202/616-6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Claimant on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC-27

System name:

Germany, Holocaust Survivors' Claims Against.

System location:

Foreign Claims Settlement Commission, 600 E Street, Northwest, Room 6002, Washington, DC 20579.

Categories of individuals covered by the system:

Natural persons who assert claims for loss of liberty or damage to body or health as a result of National Socialist measures of persecution conducted directly against them.

Categories of records in the system:

Claim information, including name and address of claimant and representative, if any; date of birth or naturalization; nature and valuation of claim, including description of measures of persecution; other evidence establishing entitlement to compensation for claim.

Authority for maintenance of the system:

Pub. L. 104-99, and the Agreement Between the Government of the United States of America and the Government of the Federal Republic of Germany Concerning Final Benefits to United States Nationals Who Were Victims of National Socialist Measures of Persecution, September 19, 1995.

Purpose(s):

To enable the Commission to carry out its statutory responsibility to determine the valid amount of the claims before it.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromise

information; and (3) the disclosure made to such agencies, entities, and persons is reasonable and necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee if such communication may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Records were used for the purpose of determining the validity and amount of claims; issuance of decisions concerning eligibility to receive compensation under the claims statute and the Claims Agreement; notifications to claimants of rights to appeal; preparation of decisions for certification to the Secretary of State for use in diplomatic settlement negotiations with Germany; and preparation of certifications of awards to the Secretary of the Treasury for payment. Names and other information furnished by claimants may be used for verifying citizenship status with the INS. As required by the authorizing statute, the information contained in this system of records will be maintained as confidential information which is exempt from disclosure to the public.

—Law Enforcement: In the event that a system of records maintained by the FCSC to carry out its functions indicates a violation or potential violation of law, whether civil or criminal or regulatory in nature and whether arising by general statute or particular program statute or order issued pursuant thereto, the relevant records in the system of records may be referred to for use as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with enforcing or implementing the statute, rule, regulation or order issued pursuant to the

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or

iii. Any employee of the FCSC in his or her official capacity where the Department of Justice has agreed to represent the employee, or

iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by claim number. Alphabetical index used for identification of claim.

Safeguards:

At FCSC: Building employees security guards. Records are maintained in a locked room accessible to authorized FCSC personnel and other persons when accompanied by security personnel.

Retention and disposal:

Records are maintained in accordance with 5 U.S.C. 301. Disposal of records will be in accordance with 44 U.S.C. 3301–3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Officer, Foreign Claims Settlement Commission, 600 E Street, NW., Room 5000, Washington, DC 20579; telephone 202–616–6975, fax 202–616–6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Claimant on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC-28

System name:

Iraq, Registration of Potential Claims Against.

System location:

Foreign Claims Settlement Commission, 600 E Street NW, Room 6002, Washington, DC 20579.

Categories of individuals covered by the system:

Natural and juridical persons with potential claims against Iraq that are outside the juris of the United Nations Compensation Commission.

Categories of records in the system:

Claim information, including name and address of claimant and representative, if any; d place of birth or naturalization; nature and valuation of claim, including description of pr or other asset or interest that is the subject of the claim; other evidence establishing entitlement to compensation for claim.

Authority for maintenance of the system:

Information in the system was collected under the Foreign Claims Settlement Commission's general authority to adjudicate claims conferred by 22 U.S.C. 1621 et seq.

Purpose(s):

To enable the Commission to formulate recommendations concerning the drafting of legislation to authorize formal adjudication of claims against Iraq.

Routine uses of records maintained in the system, including categories of users and purposes of the uses:

To appropriate agencies, entities, and persons when (1) The Commission suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Commission's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The Commission may disclose relevant and necessary information to a former employee of the Commission for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department of Justice regulations; or facilitating communications with a former employee if such disclosure may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

—Records are used for the purpose of determining the validity and amount of potential claims to facilitate planning for adjudication of such claims in the future. Names and other information furnished by registrants may be used for verifying citizenship status with the INS. Name and addresses of individual registrants will be subject to public disclosure. Other information provided by the individual registrants will be maintained as confidential information which will be exempt from disclosure to the public.

—Law Enforcement: In the event that a system of records maintained by the FCSC to c

its functions indicates a violation or potential violation of law, whether civil or criminal or regulatory in nature and whether arising by general statute or particular program statute or order issued pursuant thereto, the relevant records in the system of records may be referred as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with enforcing or implementing the statute, rule, regulation or order issued pursuant to the

—A record, or any facts derived therefrom, may be disclosed in a proceeding before a court or an adjudicative body before which the FCSC is authorized to appear or to the Department of Justice for use in such proceeding when:

- i. The FCSC, or any subdivision thereof, or
- ii. Any employee of the FCSC in his or her official capacity, or
- iii. Any employee of the FCSC in his or her official capacity where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the FCSC determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records determined by the FCSC to be arguably relevant and necessary to the litigation and such disclosure is determined by the FCSC to be a use compatible with the purpose for which the records were collected.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records maintained in file folders.

Retrievability:

Filed numerically by registration number. Alphabetical index used for identification of records.

Safeguards:

At FCSC: Building employs security guards. Records are maintained in a locked room.

accessible to authorized FCSC personnel and other persons when accompanied by such personnel.

Retention and disposal:

Records are maintained in accordance with 5 U.S.C. 301. Disposal of records will be in accordance with 44 U.S.C. 3301–3314 when such records are determined no longer useful.

System manager(s) and address:

Administrative Officer, Foreign Claims Settlement Commission, 600 E Street, NW, Room 6002, Washington, DC 20579; telephone 202–616–6975, fax 202–616–6993.

Notification procedure:

Set forth in part 504 of title 45, Code of Federal Regulations.

Contesting record procedures:

Same as above.

Record source categories:

Registrant on whom the record is maintained.

[\[TOP\]](#)

JUSTICE/FCSC–29

SYSTEM NAME:

Libya, Claims Against.

SYSTEM LOCATION:

Offices of the Foreign Claims Settlement Commission, 600 E Street, NW., Suite 6002, Washington, DC 20579.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Persons with claims against Libya covered by the August 14, 2008 Claims Settlement Agreement Between the United States of America and the Great Socialist People's Libyan Arab Jamahiriya and referred by the Department of State to the Foreign Claims Settlement Commission.

CATEGORIES OF RECORDS IN THE SYSTEM:

Claim information, including name and address of claimant and representative, if any; date of birth or naturalization; nature of claim; description of loss or injury including medical records; and other evidence establishing entitlement to compensation.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority to establish and maintain this system is contained in 5 U.S.C. 301 and 44 U.S.C. 3101, which authorize the Chairman of the Commission to create and maintain federal records of agency activities, and is further described in 22 U.S.C. 1622e, which vests all non-adjudicatory functions, powers and duties in the Chairman of the Commission.

PURPOSE:

To enable the Commission to carry out its statutory responsibility to determine the valid amount of certain claims of U.S. nationals against Libya.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

The information contained in this system of records will be disclosed by the Commission in the following circumstances:

- a. To the Department of State and the Department of the Treasury in connection with the negotiation, adjudication, settlement and payment of claims;
- b. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government.

government, when necessary to accomplish a Commission function related to this system's records;

c. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

d. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

e. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice and/or the Commission determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

f. To a former employee of the Commission for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Commission regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Commission requires information and/or consultation from the former employee regarding a matter within that person's former area of responsibility.

g. To appropriate agencies, entities, and persons when (1) it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised and the Commission has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Commission or another agency or entity) that rely upon the compromised information; and (2) the disclosure made to such agencies, entities, and persons is reasonably necessary to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

STORAGE:

Paper records maintained in file folders at the Commission's office and an electronic Microsoft Access database located on the Commission's Server.

RETRIEVABILITY:

Information from this system of records will be retrieved by claimant name, claim number and/or decision number. An alphabetical index is used for identification of a claim by claimant name (see system "Justice/FCSC-1" originally published in the *Federal Register*, June 1999, 64 FR 31296).

SAFEGUARDS:

Paper records are under security safeguards at the Commission's office. The electronic records are safeguarded by the DOJ JCON security procedures. Access to the Commission's database requires a password and is limited to Commission employees and contractors with appropriate security clearances.

RETENTION AND DISPOSAL:

Records are maintained under 5 U.S.C. 301. Disposal of records will be in accordance with determination by the National Archives and Records Administration with regard to the Commission's request for Records Disposition Authority dated November 26, 2008.

SYSTEM MANAGER(S) AND ADDRESS:

Administrative Office, Foreign Claims Settlement Commission, 600 E Street, NW., Suite 1000, Washington, DC 20579. Telephone: 202/616-6975. Fax: 202/616-6993.

NOTIFICATION PROCEDURE:

The Administrative Officer will inform any person or other agency about any correction or notation of dispute made in accordance with title 45 CFR Sec. 503.7 of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

RECORD ACCESS PROCEDURE:

(a) Upon request in person or by mail, any individual will be informed whether or not a record exists.

of records maintained by the Commission contains a record or information pertaining to individual. (b) Any individual requesting access to a record or information on himself or herself must appear in person at the offices of the Foreign Claims Settlement Commission, 600 E Street, NW., Room 6002, Washington, DC, between the hours of 9 a.m. and 5 p.m., Monday through Friday, and (1) Provide information sufficient to identify the record, e.g., the individual's own name, claim and decision number, date and place of birth, etc.; (2) Provide identification sufficient to verify the individual's identity, e.g., driver's license, identification or Medicare card; and (3) Any individual requesting access to records or information pertaining to himself or herself may be accompanied by a person of the individual's own choosing while reviewing records or information. If an individual elects to be so accompanied, advance notification and election will be required along with a written statement authorizing disclosure and discussion of the record in the presence of the accompanying person at any time, including the time access is granted. (c) Any individual making a request for access to records or information pertaining to himself or herself by mail must address the request to the Administrative Officer (Privacy Officer), Foreign Claims Settlement Commission, 600 E Street, NW., Room 6002, Washington, DC 20579, and must provide information acceptable to the Administrative Officer to verify the individual's identity. (d) Responses to requests under this section normally will be made within ten (10) days of receipt (excluding Saturdays, Sundays, and legal holidays). If it is not possible to respond to requests within that period, an acknowledgment will be sent to the individual within ten (10) days of receipt of the request (excluding Saturdays, Sundays, and legal holidays).

CONTESTING RECORD PROCEDURES:

(a) Any individual may request amendment of a record pertaining to himself or herself according to the procedure in paragraph (b) of this section, except in the case of record described under paragraph (d) of this section. (b) After inspection by an individual of a record pertaining to himself or herself, the individual may file a written request, presented in person or by mail, with the Administrative Officer, for an amendment to a record. The request must specify the particular portions of the record to be amended, the desired amendments and the reasons therefor. (c) Not later than ten (10) days (excluding Saturdays, Sundays, and legal holidays) after the receipt of a request made in accordance with this section to amend a record in whole or in part, the Administrative Officer will: (1) Make any correction of any portion of the record which the individual believes is not accurate, relevant, timely or complete and then inform the individual of such correction; or (2) Inform the individual, by certified mail return receipt requested, of the refusal to amend the record, setting forth the reasons therefor, and notify the individual of the right to appeal that determination as provided under 45 CFR

503.8. (d) The provisions for amending records do not apply to evidence presented in the course of Commission proceedings in the adjudication of claims, nor do they permit collateral attack upon what has already been subject to final agency action in the adjudication of claims in programs previously completed by the Commission pursuant to statutory time limitations.

RECORD SOURCE CATEGORIES:

Claimant on whom the record is maintained.

[\[TOP\]](#)

Foreign Terrorist Tracking Task Force

JUSTICE/FTTTF-001

System name:

Flight Training Candidates File System, FTTTF-001.

System location:

Foreign Terrorist Tracking Task Force (FTTTF), U.S. Department of Justice, Washington, D.C. 20530

Categories of individuals covered by the system:

Aliens and persons designated by the Under Secretary of Transportation for Security, U.S. Department of Transportation, pursuant to section 113 of the Aviation and Transportation Security Act (ATSA) who are seeking training from a Federal Aviation Administration (FAA) certificated instructor in the operation of any aircraft with maximum certificated takeoff weight of 12,500 pounds or more ("flight training candidates"); flight instructors who wish to provide such training ("providers").

Categories of records in the system:

Flight training candidate applications and identifying information contained therein (e.g., date of birth, place of birth, country of residence, education, travel, etc.); authorizations for release of information; basic identifying information of providers (e.g., name, address,

telephone number, FAA certification number); classified risk assessment reports; record received from the Federal Bureau of Investigation regarding the results of its fingerprint name checks of the flight training candidate; and electronic copies of correspondence to training candidates, providers, the Immigration and Naturalization Service and the Department of State advising them as to whether individual candidates have been determined to pose a threat to aviation or national security.

Authority for maintenance of the system:

Section 113 of the Aviation and Transportation Security Act, Pub. L. 107–71, codified at U.S.C. 44939; Homeland Security Presidential Directive-2, October 29, 2001, "Combating Terrorism Through Immigration Policies."

Purpose(s):

The system will be used to collect information and conduct the risk assessments required under section 113 of ATSA.

Routine Uses of Records Maintained in the system, including categories of users and Purpose of Such Uses:

Information may be disclosed from this system as follows:

- A. To flight training providers and other entities or persons in order to verify information submitted by individual candidates, and to facilitate the necessary risk assessment.
- B. To the United States Department of State or other federal entities concerned with visa and immigration matters for purposes of visa or status determinations and other risk warning assessment programs administered by such Department or entities.
- C. In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, or tribal law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.
- D. In an appropriate proceeding before a court or administrative or regulatory body where the information is relevant.

records are determined by the Department of Justice to be arguably relevant to the proceeding.

E. To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

F. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

G. To officials and employees of a federal agency or entity, including the White House, requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance of a security clearance; the execution of a security or suitability investigation; the classification of a job; or the issuance of a grant or benefit.

H. To federal, state, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

I. To a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

J. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

K. To the General Services Administration and National Archives and Records Administration for records management inspections conducted under the authority of 44 U.S.C. 2904 and

L. To a former employee of the Department for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding

matter within that person's former area of responsibility.

M. To such recipients and under such circumstances and procedures as are mandated federal statute or treaty.

Policies and practices for storing, retrieving, accessing, Retaining and Disposing of in the system:

Storage:

All data in this system is maintained solely in electronic form.

Retrievability:

Data is retrieved by the name of the flight training candidate or the provider.

Safeguards:

Information in this system is safeguarded in accordance with applicable rules and policies including the Department's automated systems security and access policies. Classified information is appropriately stored in secure facilities, databases, and containers and in accordance with other applicable requirements. In general, records and technical equipment are maintained in buildings with restricted access. The required system protection method also restricts access. Access is limited to those who have a need for access to perform their official duties.

Retention and disposal:

Records concerning an individual will be deleted from the system when: (a) The individual reaches 99 years of age or 5 years have elapsed since a report of the individual's death when no longer needed for reference, whichever is sooner (pending approval of the Arc the United States).

System manager(s) and address:

Director, Foreign Terrorist Tracking Task Force, Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530.

Notification procedures:

Address inquiries to the System Manager named above.

Record access procedures:

Any flight training candidate or provider who submits information into the system will be able to view online the information they submit through the use of a password. U.S. citizens and Permanent Resident Aliens may seek access to additional information about a request for flight training by writing to the System Manager listed above. The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury. Some information may be exempt from access as described in section entitled "Systems Exempted from Certain Provisions of the Act." A determination as to whether a record may be accessed will be made at the time a request is received.

Contesting record procedures:

U.S. Citizens or Permanent Resident Aliens who wish to contest, or seek amendment of information maintained in the system should direct their requests to the System Manager listed above. Requests should clearly and concisely state what information is being contested, the reason(s) for contesting it, and the proposed amendment to the record. Some information may be exempt from amendment and contesting record procedures as described in the section entitled "Systems Exempted from Certain Provisions of the Act." A determination as to whether a record may be amended will be made at the time a request is received.

Record source categories:

Information in this system of records will be obtained from flight training candidates; persons and individuals or entities having information pertinent to the determination of risk to aviation and national security, including but not limited to purveyors of public source data, government entities, and the FAA.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3), (d)(1), (2), (3) and (e)(1) and (4)(I) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1). This exemption

only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(k)(1).

Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

Immigration and Naturalization Service

JUSTICE/INS-005

System name:

INS Image Storage and Retrieval System (ISRS).

System location:

Headquarters, Regional Offices, Administrative Centers, Service Centers, District Offices of Entry, and file control offices of the Immigration and Naturalization Service in the United States as detailed in JUSTICE/INS-999, last published, April 13, 1999 (64 FR 18052). Offices having access to the system are: The Law Enforcement Support Center, 188 Hall Lane, Williston, Vermont 05495; the Central States Command Center, 10 West Jackson Boulevard, Chicago, Illinois 60604; and the Forensic Document Laboratory, 8000 Westp Drive, Suite 325, McLean, Virginia 22101-3105.

Categories of individuals covered by the system:

Persons lawfully admitted for permanent residency; Asylees and Parolees lawfully admitted for employment authorization (although, Asylees and Parolees are not initially covered under the Privacy Act, these individuals often change their status to lawful permanent residents at that time and will be covered by the Privacy Act); Commuters and other persons authorized for frequent border crossing; Naturalized United States Citizens.

Categories of records in the system:

Records consist of formatted data base records of personal biographical data including: date of birth, mother's first name, father's first name, and country of birth; and biometric

information (i.e., fingerprints, digital images of facial picture, and signatures).

Authority for maintenance of the system:

8 U.S.C. 1103, 1321, and 1360.

Purpose(s):

This system of records is used: To verify controlled INS documents issued to individuals covered by the system; to assist the INS with its responsibility to detect and reduce fraud entry to the United States; and to detect and reduce the proliferation of fraudulent INS documents.

Routine uses of records maintained in the system, including categories of users and purpose of such uses:

Relevant information contained in this system of records may be disclosed as follows:

A. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

B. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record.

C. To the General Services Administration and National Archives and Records Administration records management inspections conducted under the authority of 44 U.S.C. 2904 and

D. To the appropriate agency/organization/task force, regardless of whether it is Federal, local, foreign, or tribal, charged with the enforcement (e.g., investigation and prosecution of law (criminal or civil), regulation, or treaty, of any record contained in this system of records which indicates either on its face, or in conjunction with other information, a violation or potential violation of that law, regulation, or treaty.

E. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal

government, when necessary to accomplish an agency function related to this system c records.

F. Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

INS Image Storage and Retrieval System (ISRS) information is stored on magnetic media (internal image server disk drives).

Retrievability:

Individual records are indexed and retrievable by name, alien registration number (A-number), and application receipt number. In cases where an individual record can not be retrieved using one of these key indexes, combinations of multiple data elements may be used (e.g. name, date of birth, and country of birth) if necessary, to assist in the identification and retrieval of a unique record.

Safeguards:

Most INS offices are located in buildings under security guard, with access limited to INS and other Federal Government employees and authorized visitors. All records are stored in secure facilities which are locked outside of normal office hours at the Department of Justice Data Center. Automated equipment is physically accessible only by authorized Department of Justice personnel. Electronic access to the automated system is controlled by restricted password use at remote terminals in secured areas.

Retention and disposal:

Image Storage and Retrieval System data records are retained in the system for a period of 5 years and then destroyed.

System manager(s) and address:

Associate Commissioner, Immigration Resources Management, Immigration and Naturalization Service, 800 I Street, NW., Room 700, Washington, DC 20536.

Notification procedure:

Inquiries should be addressed to the system manager at the INS office where the record is maintained or (if unknown) to the FOIA/PA Officer, INS, 425 I Street NW., Second Floor Labor Life Building, Washington, DC 20536.

Record access procedure:

Requests for access to records in this system shall be in writing and should be addressed to the System Manager noted above or to the appropriate FOIA/PA Officer as indicated in the System Locations. Requests sent directly to the System Manager should be submitted by mail. Requests to the FOIA/PA Officer may be submitted by mail. Requests to the FOIA/PA Officer may be submitted either by mail or in person. If a request for access is made by mail, the envelope and letter shall be clearly marked Privacy Access Request. Include a description of the general subject matter and if known, the related file number. To identify a record, the requester should provide his or her full name, date and place of birth, verification of identity in accordance with 8 CFR 103.21(b) or provide a statement under penalty of perjury, alien number, the date and place of entry into or departure from the United States and any other identifying information which may be of assistance in locating the record. The requester should also provide a return address for transmitting the records to be released.

Contesting record procedures:

An individual desiring to request amendments of records maintained in this system should direct his or her request to the System Manager or to the appropriate FOIA/PA Officer in the System Locations. The request should state the information being contested, the reasons for contesting it, and the proposed amendment thereof. Persons filing such requests should enclose the envelope with the following legend Privacy Act Amendment Request.

Record source categories:

Basic information contained in this INS data repository is supplied by aliens wishing to seek entry to the United States and/or those already in the United States seeking benefits from Immigration and Naturalization Service. External entities including Department of State overseas consular offices and United States embassies and the Department of Labor may provide data on individuals seeking entry into the United States.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/INS-007

System name:

Orphan Petitioner Index and Files.

System location:

Headquarters, District offices and suboffices of the Immigration and Naturalization Service (Service) in the United States and foreign countries, as detailed in JUSTICE/INS-999, last published in the *Federal Register* on April 13, 1999 (64 FR 18052).

Categories of individuals covered by the system:

Individuals who are prospective petitioners or who have filed an application for Advance Processing of Orphan Petition under the Immigration and Nationality Act, as amended.

Categories of records in the system:

The system contains form I-600A, Application for Advance Processing of Orphan Petition for advance processing of orphan petitions by prospective adoptive parent(s); documents of prospective adoptive parent(s)' United States citizenship and marital status, agency responses indicating whether prospective adoptive parent(s) have any arrest records; and home study

which include statements of financial ability and other elements that relate to the ability prospective adoptive parents to provide proper care to beneficiary orphans.

Authority for maintenance of the system:

8 U.S.C. 1103 and 1154; and 42 U.S.C. 14901.

Routine uses of records maintained in the system, including categories of users and PURPOSE OF SUCH USE:

Information in the system will be used by employees of the Immigration and Naturalization Service to determine the status of pending requests or petitions, to locate related files and other records promptly, and to determine the suitability of prospective petitioners as adoptive parents. Information regarding the status and progress of cases and the suitability of prospective petitioners as adoptive parents may be disseminated to other components of the Department of Justice, Members of Congress, and the President. In addition:

- A. Relevant information from this system may be referred to the Department of State in processing of petitions or issuance of visas for benefits under the Immigration and Nationality Act, as amended.
- B. Information from this system may be referred to officials of other federal, state and local government agencies and adoption agencies and social workers to elicit information required for making a final determination of the petitioner's ability to care for a beneficiary orphan.
- C. To an attorney or representative who is acting on behalf of an individual covered by this system of records as defined in 8 CFR 1.1(j) in conjunction with any proceeding before the Immigration and Naturalization Service or the Executive Office for Immigration Review.
- D. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.
- E. To a Member of Congress, or staff acting upon the Member's behalf, when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record.

F. To the General Service Administration (GSA) and the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

G. To contractors, grantees, experts, consultants, students and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

H. To a court of adjudicative body before which the appropriate DOJ component is authorized to appear when any of the following is a party to litigation or has an interest in litigation in which such records are determined by the appropriate DOJ component to be arguably relevant to the litigation:

- (1) The DOJ component, or any subdivision thereof, or
- (2) Any employee of the DOJ in his or her official capacity, or
- (3) Any employee of the DOJ in his or her individual capacity where the DOJ has agreed to represent the employee or has authorized a private attorney to represent him or her, and
- (4) The United States, where the DOJ determines that the litigation is likely to affect it or its subdivisions.

I. Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records are maintained as paper records in file folders.

Retrievability:

Records are retrieved by the name of the petitioner.

Safeguards:

Most INS offices are located in buildings under security guard, with access limited to INS and other Federal Government employees and authorized visitors. All records are stored in locked cabinets which are locked outside of normal office hours.

Retention and disposal:

Records from the advance processing file folders are retained for one year after the completion of all advance processing. After one year the records are returned to the petitioner or the responsible state or licensed agency. Materials which cannot be returned to the petitioner or responsible state or licensed agency will be destroyed.

System manager(s) and address:

Associate Commissioner, Examinations, Immigration and Naturalization Service, 425 I Street NW, Washington, DC 20536.

Notification procedure:

Inquiries should be addressed to the District Director or Officer in Charge of the Service where the file is located. If the file location is not known, inquiries may be addressed to the System Manager, as noted above. To enable the Service to identify whether the system contains a record relating to an individual, the requester must provide the individual's full name, date of birth, place of birth, and a description of the subject matter.

Record access procedure:

A person desiring access to a record shall submit a request in writing to the agency official designated under "Notification Procedure" above. The requester must also identify the record by furnishing the information listed under that caption. If a request to access a record is

by mail, the envelope and letter shall be clearly marked "Privacy Act Request," and a return address must be provided for transmitting any information.

Contesting record procedure:

An individual desiring to request amendment of records maintained in this system of records should direct his or her request to the System Manager or to the appropriate FOIA/PA Component noted in System Locations. The request should state the information being contested, the reason(s) for contesting it, and the proposed amendment thereof. Persons filing such requests should mark the envelope with the following legend "Privacy Act Amendment Request."

Record source categories:

Information in the system is obtained from requests and petitions filed by the petitioners and private adoption agencies and social workers; and federal, state, local and foreign government agencies.

Systems exempted from certain provisions of the act:

This system is exempt from subsection (d) of the Privacy Act. This exemption applies to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a. INS has published implementing regulations in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and these have been published in the *Federal Register*. See 28 CFR 16.99(e).

[\[TOP\]](#)

JUSTICE/INS-011

System name:

Password Issuance and Control System (PICS).

System location:

Central, Regional, and District offices of the Immigration and Naturalization Service (INS) detailed in JUSTICE/INS-999.

Categories of individuals covered by the system:

Those INS employees, INS contractor employees, and other Federal, State or local government employees for whom authorization to access and use INS automated data processing (ADP) systems has been requested.

Categories of records in the system:

This system of records consists of paper records (INS Form G-872, Request for ADP Password) and an automated data base. INS Form G-872 contains personal identification information such as name, social security number, office location code, organization code, ADP security clearance information, office telephone number, company name of contractor employee and a statement by the supervisor certifying the official need for access. Upon approval of the request, the user ID code and password issued will be included on the Form. The automated data base may include information extracted from INS Form G-872 and from the Security Clearance Information System (SCIS), JUSTICE/JMD-008. The SCIS data is necessary to determine the suitability and trustworthiness to access the information.

Authority for maintenance of the system:

Section 103 of the Immigration and Nationality Act (8 U.S.C. 1103) as amended by section 101 of the Immigration Reform and Control Act of 1986 (8 U.S.C. 1324) and Department of Justice Order 2640.2A which delegates ADP security authority to INS for maintaining and operating ADP systems.

Purpose(s):

The purpose of the system is to expedite determinations of eligibility to access INS automated data processing systems and to improve control by ADP Security Officers of ADP password and user ID distribution.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant information contained in this system of records may be disclosed as follows:

A. Where there is an indication of violation or potential violation of law (whether civil, criminal or

regulatory in nature), to the appropriate agency (whether Federal, State, local or foreign charged with the responsibility of investigating or prosecuting such violations, or charge enforcing or implementing the statute, rule, regulation or order issued pursuant thereto.

B. To the General Services Administration and the National Archives and Records Administration in records management inspections conducted under the authority of 44 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

To contractors, grantees, experts, consultants, students, and others performing or working under a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Those records which can be accessed electronically are stored in a database on magnetic tape. Forms G-872, Request for ADP Password, are maintained in file folders at Central, Regional, and District ADP Security Offices.

Retrievability:

These records are retrieved by social security number.

Safeguards:

INS offices are located in buildings under security guard, and access to premises is by

identification. Paper records are stored in locked files during non-duty hours. Access to automated data is obtained through terminals which require the use of restricted password and user IDs. Only designated Security Officers have access to PICS for creating and updating records of users within their jurisdiction.

Retention and disposal:

Inactive automated records are retained 10 years after date of last action and then deleted from the system. INS Forms G-872, Request for ADP Password, are retained 3 years after final action and then destroyed by shredding.

System manager(s) and address:

The Servicewide system manager is the Director, Technical Services Branch, Data Systems Division, Immigration and Naturalization Service, 425 I Street NW, Washington, DC 20535.

Notification procedure:

Address inquiries to the system manager identified above.

Record access procedures:

Make all requests for access in writing to the Freedom of Information Act/Privacy Act (FOIA/PA) Officer at the address identified above. Clearly mark the envelope and letter "Privacy Act Request." Provide the full name, social security number, user ID, and notarized signature of the individual who is the subject of the record, and a return address.

Contesting record procedures:

Direct all requests to contest or amend information to the FOIA/PA Officer at the address identified above. State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment thereof. Clearly mark the envelope "Privacy Act Request." The record must be identified in the same manner as described for making a request for access.

Record source categories:

INS Form 872, Request for ADP Password, completed by the supervisor or program manager.

and security clearance information extracted from SCIS, JUSTICE/JMD-008.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/INS-015

System name:

Port of Entry Office Management Support System (POMS).

System location:

Port of entry inspection facilities under the District Offices of the Immigration and Naturalization Service (INS) in the United States as detailed in JUSTICE/INS-999.

Categories of individuals covered by the system:

INS employees assigned inspection duties at United States ports of entry.

Categories of records in the system:

Personal identification information, e.g., name, address, social security number, identification and stamp inspection numbers assigned to the inspectors; personnel-related data, e.g., personnel files and position titles, classification, step and grade; and resource management records, e.g., work schedules, including leave and overtime worked, and costs data, including dollars allocated to regular and overtime pay.

Authority for maintenance of the system:

5 U.S.C. chapters, 53, 54, 61, 63; 8 U.S.C. 1103; and 44 U.S.C. 3101.

Purpose(s):

The information in this system will be used to assist management in scheduling leave, in

assigning and controlling overtime, in accounting for use of overtime funds, and in the management of resources at the various ports of entry.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

There are no routine uses. Information will be accessible only to management, administrative and operational personnel at a given port who need the information for port management and reporting.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

To contractors, grantees, experts, consultants, students, and others performing or working under a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system and its records.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

These records are stored on hard disk and diskette.

Retrievability:

These records are retrieved by name and identification number.

Safeguards:

INS offices are located in buildings under security guard and access to the premises is

official identification. Access to records is restricted to INS employees through the use of identification and password levels.

Retention and disposal:

These records are maintained 90 days after the employee is separated or transferred from port and then deleted from the system.

System manager(s) and address:

Assistant Commissioner, Inspections, 425 I Street, NW, Washington, DC 20536.

Notification procedure:

Address inquiries to Port Supervisor or System Manager identified above.

Record access procedures:

Make all requests for access in writing to the Freedom of Information Act/Privacy Act (FOIA/PA) Officer at the nearest INS office, or the INS office maintaining the desired records (if known) using the list of principal offices of the Immigration Naturalization Service Appendix, JUSTICE/INS-999, published in the *Federal Register*. Clearly mark the envelope and letter "Privacy Act Request." Provide the full name and date of birth, with a notarized signature of the individual who is the subject of the record, and a return address.

Contesting record procedures:

Direct all requests to contest or amend information in the record in writing to the FOIA/PA Officer at one of the addresses identified above. State clearly and concisely the information being contested, the reason for contesting it, and the proposed amendment thereof. Clearly mark the envelope "Privacy Act Amendment Request." The record must be identified in the same manner as described for making a request for access.

Record source categories:

The sources of information for POMS will be the employee and personnel management records.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/INS-016

System name:

Secondary Verification Automated Log (SVAL).

System location:

Headquarters. Regional, District, and other offices of the Immigration and Naturalization Service (INS) in the United States as detailed in JUSTICE/INS-999.

Categories of individuals covered by the system:

Immigrant aliens apply for Federal entitlements for whom INS receives a Form G-845, Document Verification request, which is submitted by Federal and State entitlements agencies.

Categories of records in the system:

Temporary paper records include Form G-845 as submitted by the entitlement agency. These records contain the following data: Alien name and identifying number, name of the entitlement agency, and immigration status as reported by the alien applicant. INS will update Form G-845 with immigration status information and return it to the entitlement agency. However, identification data, together with Form G-845 disposition data, will be recorded and maintained by INS on hard and floppy disks as a record of secondary verifications made by the entitlement agency.

Authority for maintenance of the system:

8 U.S.C. 1255a, 8 U.S.C. 1324a, 8 U.S.C. 1360 and 42 U.S.C. 1320b-7.

Purpose(s):

The SVAL JUSTICE/INS-016 system is used to maintain records of a second attempt by entitlement agencies to verify immigration status by comparing paper documents (known as the "secondary verification"). Secondary verification is conducted where eligibility for certain benefits was not or could not be confirmed through direct access to an INS automated database entitled "Alien Status Verification Index" (ASVI), JUSTICE/INS-009 (known as "primary verification"). Specifically, INS is asked to compare the entitlement agency's paper record, Form G-845 (which contains information provided by the immigrant aliens applying for Federal entitlements), with INS paper records; complete the Form relative to immigration status; and return it to the entitlement agency. The SVAL, JUSTICE/INS-016 system is maintained to track the interim and final disposition of the second request to verify eligibility which may require referral to an INS district office.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant information contained in this system of records may be disclosed to the following:

- A. To a Federal, State, or local government agency in response to a request for information regarding the status and/or disposition of a document verification request submitted by that agency.
- B. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record.
- C. To the General Services Administration and the National Archives and Records Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Until they have been processed and returned to the entitlement agency, Forms G-845 are stored in a card index file. Data extracted from the form is stored in personal computers on hard and floppy disks.

Retrievability:

These records are retrieved by serial number, A-file number and/or name of immigrant applicant.

Safeguards:

INS offices are located in buildings under guard and access to the premises is by official identification. Access to personal computers is limited to INS employees and access to data in this system is further restricted through user identification and discrete password functions to assure that accessibility is limited.

Retention and disposal:

Form G-845 is retained long enough to complete the verification, at which time the form is returned to the entitlement agency. Completed verifications are archived on disk monthly and destroyed five (5) years after the last month contained on the disk. Disposition authority is INS Disposition Schedule NI-85-90-3.

System manager(s) and address:

Assistant Commissioner, Office of Records, Office of Examinations, Immigration and Naturalization Service, 425 I Street NW, Washington, DC 20536.

Notification procedures:

Address your inquiries about the system in writing to the system manager identified above.

Headquarters, Regional, District, and other offices of the Immigration and Naturalization Service (INS) in the United States as detailed in JUSTICE/INS—999.

Categories of individuals covered by the system:

INS employees who are responsible for the procurement and management of automate processing equipment (ADPE); and, contractors who have been assigned ADPE to use developing software programs for INS.

Categories of records in the system:

An inventory reflecting (1) the ADPE procurement and management activities of INS em and (2) the identity of contractors using such equipment to develop software programs : The inventory will include information relating to the kinds and quantity of ADPE equipn procured, the disposition of such equipment and the purpose for such disposition, and/ (where appropriate) information relating to the reassignment of responsibility for the equipment. Such reassignment may be made based upon the resignation or transfer of responsible employees, upon the expiration of the subject contracts, or otherwise upon need to track the status or disposition of the equipment and identify the management employee responsible therefor, e.g., removal of the equipment from the inventory for rep purposes. Records will include identifying information such as INS employee or contrac name/title, social security number, office location/address and phone number, company of the contractor, and other relevant information such as the level of responsibility assign the INS employee.

Authority for maintenance of the system:

8 U.S.C. 1103 and 40 U.S.C. 483.

Purpose(s):

To provide accountability records relating to (1) INS employee management and dispos ADPE equipment and (2) contractor use of such equipment in developing software prog for INS. The records will be used by management to track and account for the procurer and disposition of all ADPE, and thus ensure the integrity and security of the ADPE inv

Routine uses of records maintained in the system, including categories of users and

purposes of such uses:

Relevant information contained in this system of records may be disclosed as follows:

- A. Where there is an indication of a violation or potential violation of law (whether civil, criminal or regulatory in nature), to the appropriate agency (whether Federal, State, local or foreign) charged with the responsibility of investigating or prosecuting such violations, or charge enforcing or implementing the statute and/or the rule, regulation or order issued pursuant thereto.
- B. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record.
- C. To the General Services Administration and the National Archives and Records Administration in records management inspections conducted under the authority of 44 CFR 2904 and 2906.
- D. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:***Storage:***

The records are stored in a data base on magnetic disk.

Retrievability:

These records may be retrieved by INS employee and contractor name, machine serial number, company name, or office location.

Safeguards:

The records are accessed from mainframe computer terminals located in INS offices throughout the country.

locked during non-duty hours. Access is obtained through terminals which require the use of restricted passwords and user identification numbers. Only designated personnel have access to AIMS for creating and updating ADPE Inventory records within their jurisdiction.

Retention and disposal:

A schedule for the retention and disposal of these records is under review and development.

System manager(s) and address:

The Servicewide system manager is the Associate Commissioner, Information Resource Management, Immigration and Naturalization Service, 425 I Street, NW, Washington, DC 20536.

Notification procedures:

Address your inquiries to the system manager identified above.

Record access procedures:

Make all requests for access in writing to the Freedom of Information Act/Privacy Act (FOIA/PA) Officer at the address identified above. Clearly mark the envelope and letter "Privacy Act Request." Provide the full name, social security number, user identification number, and notarized signature of the individual who is the subject of the records, and a return address.

Contesting record procedures:

Direct all requests to contest or amend information to the FOIA/PA Officer at the address identified above. State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment thereof. Clearly mark the envelope and letter "Privacy Act Request." The record must be identified in the same manner as described when making a request for access.

Record source categories:

The individuals covered by the system are the record sources.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/INS-020

System name:

Finance Section Indexes.

System location:

Headquarters, Regional and District offices, Administrative Centers, Service Centers, and file control offices of the Immigration and Naturalization Service (INS) in the United States are detailed in JUSTICE/INS-999.

Categories of individuals covered by the system:

Creditors and debtors, including:

- (a) Individuals who are indebted to the United States Government, whether it be for goods or services, or benefits, or for administrative fines and assessments, etc.
- (b) Employees who have received travel advances or overpayments from the United States Government, who are in arrears in their accounts, or who are liable for damage to Government property.
- (c) Vendors who have furnished supplies, material, equipment, and/or services to the Government.
- (d) Employees and witnesses who have performed official travel.
- (e) Employees and other individuals who have a claim against the Government.

Categories of records in the system:

Accounts with creditors—Records include vendors' invoices, purchase orders, travel vouchers, and claims.

Accounts with debtors—Records include bills for inspection services performed under the Immigration and Naturalization Act of March 2, 1931; fees, fines, penalties, vendor indebtedness for overpayments, and deportation expenses assessed pursuant to the Immigration and Nationality Act; and employee indebtedness for travel advances, for the unofficial use of Government facilities and services, for damage to or loss of Government property, and for erroneous or overpayment of compensation for travel expenses.

Authority for maintenance of the system:

- (1) Sec. 103, 265 and 290 and Title III of the Immigration and Nationality Act (66 Stat. 163, as amended (8 U.S.C. 1103; 8 U.S.C. 135; 8 U.S.C. 1360), and the regulations pursuant thereto;
- (2) 31 U.S.C. 66a.

Purpose(s):

This system of records is used to provide an accounting of the financial activities of the Department, including accounts receivable and accounts payable, and to assist management in the administration of these activities. Further, the system provides the necessary information to meet external fiscal reporting requirements and respond to written inquiries and complaints from the public.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant information contained in this system of records may be disclosed as follows:

A. Where the record, either on its face or in conjunction with other information, indicates a violation or potential violation of law (whether civil, criminal or regulatory in nature) to the appropriate agency, (whether federal, state, local or foreign) charged with the responsibility of investigating or prosecuting such violations or charged with enforcing or implementing the related statute, rule, regulation or order issued pursuant thereto.

B. To other Federal or State agencies as specified in applicable law or implementing regulations.

C. To the Internal Revenue Service (IRS) to obtain taxpayer mailing addresses for the purpose of locating such taxpayer to collect or compromise a Federal claim against the taxpayer. Addresses obtained from IRS may be redisclosed to consumer reporting agencies, but only for the purposes of allowing these agencies to prepare a commercial credit report for INS use.

D. To employers to effect salary or administrative offsets to satisfy a debt owed the United States by that person; or, when other collection efforts have failed, to the IRS to effect a collection against Federal income tax refund due. Such disclosures will be made only when all procedural steps (including due process) established by the Debt Collection Act have been taken.

E. To a person or organization with whom the head of the agency has contracted for collection services to recover indebtedness owed to the United States. Addresses of taxpayers obtained from the IRS will also be disclosed, but only where necessary to locate such taxpayer to collect or compromise a Federal claim.

F. To a Federal, State, local, or foreign agency or to an individual or organization if there is a reasonable reason to believe that such agency, individual, or organization possesses information relevant to the debt, the identity or location of the debtor, the debtor's ability to pay, or relating to any other matter which is relevant and necessary to the settlement, effective litigation and enforcement of collection of the debt, or relating to the civil action trial or hearing, and the disclosure is reasonably necessary to elicit such information or to obtain the cooperation of a witness or other agency.

G. In a proceeding before a court or adjudicative body before which INS or the Department of Justice (DOJ) is authorized to appear when any of the following is a party to litigation or has a direct interest in litigation and such records are determined by INS or DOJ to be arguably relevant to the litigation: The DOJ, or any DOJ component or subdivision thereof; any DOJ employee acting in his/her official capacity; any DOJ employee in his/her individual capacity where the DOJ has agreed to represent the employee; or the United States where INS or the DOJ determines that the litigation is likely to affect it or any of its subdivisions.

H. To any third party who may possess the information, such as the U.S. Post Office, State

motor vehicle administration, a professional organization, etc., to obtain a current mailing address in order to locate a debtor.

I. To an actual or potential party or to his or her attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, or informal discovery proceedings.

J. To a Federal agency in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter.

K. To Federal, State, and local licensing agencies or association which require information concerning the suitability or eligibility of an individual for a license or permit.

L. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

M. To a Member of Congress, or staff acting upon the Member's behalf, when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record.

N. To General Services Administration and National Archives and Records Administration records management inspections conducted under the authority of 44 U.S.C. 2904 and

31 U.S.C. 3711 requires that, where appropriate, the notice required by section 552(e)(4) must indicate that information in the system may be disclosed to a consumer reporting agency pursuant to subsection (b)(12). Such notice is provided as follows:

Disclosure to consumer reporting agencies:

Notice of Disclosure to Consumer Reporting Agencies Under Subsection (b)(12) of the Fair Credit Reporting Act

Records relating to the identity of debtors and the history of claims may be disseminated

consumer reporting agencies to encourage payment of the past-due debt. Such disclosures will be made only when a claim is overdue and only after due process steps have been taken to notify the debtor and give him or her a chance to meet the terms of the debt. Prior to disclosure, satisfactory assurances will be obtained from such consumer reporting agency concerning compliance by that agency with the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) and any other Federal law governing the provision of consumer credit information.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Generally, index records are recorded on cards and stored in file boxes and/or drawers. Original paper records are kept in file folders. These records are also maintained on microfiche and on computer processable storage media. Inactive files are stored at the Federal Records Center.

Retrievability:

Records are first retrieved by appropriation for the appropriate fiscal year and then by creditor/debtor name and/or social security number, as well as by vendor identification number.

Safeguards:

INS offices are located in buildings under security guard, and access to premises is by identification. All records are stored in spaces which are locked outside of normal office hours. Many records are stored in cabinets or machines which are locked outside of normal office hours. Access to automated records is controlled by restricted password for use of remote terminals in secured areas.

Retention and disposal:

Accounts with creditors and debtors are retained for two years from the close of the fiscal year to which they relate and then are transferred to Federal Records Centers for storage and disposition in accordance with General Records Schedules 6 and 7.

System manager(s) and address:

Assistant Commissioner, Office of Financial Management, Immigration and Naturalization Service

Service, 425 I Street, NW, Washington, DC 20536.

Notification procedure:

Inquiries may be addressed to the FOIA/PA Officer at the INS office where the record is maintained, or to the System Manager or the FOIA/PA Officer, at 425 I Street, NW, Washington, DC 20536.

Record access procedures:

Requests for access to records in this system must be in writing, and should be addressed to the System Manager or to the FOIA/PA Officer at the INS office where the record is maintained, or (if unknown) to the FOIA/PA officer at 425 I Street, NW, Washington, DC 20536. Such request may be submitted either by mail or in person. The envelope and letter shall be marked "Privacy Access Request." The requester should provide his or her full name, date of birth, verification of identity (in accordance with 8 CFR 103.21(b)) and return address for transmitting the records to be released. If known, the requester should also identify the month or year in which a debt was incurred, e.g., date of the invoice or purchase order.

Contesting record procedures:

Any individual desiring to contest or amend information maintained in the system should submit his or her request to the INS System Manager or the appropriate FOIA/PA officer as indicated under "Records Access Procedures." The request should state clearly what information is being contested, the reasons for contesting it, and the proposed amendment to the information.

Record source categories:

(1) Personnel who handle finance-related activities of the INS, such as payroll, contract purchasing, travel-related payments and debt collections and (2) the individuals covered by this system of records.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/INS-030

System name:

Job Swap/Job Exchange System (JOBX).

System location:

Immigration and Naturalization Service (INS) Headquarters, Regional and District Office sub-offices as detailed in JUSTICE/INS-999.

Categories of individuals covered by the system:

Individuals covered by the system would include all permanent INS employees interested in applying to transfer to an identical position at another location.

Categories of records in the system:

Records in this system of records contain personal data including social security number, name, Service Computation Date-leave, performance appraisal rating and date, home and work addresses, home and work telephone numbers, title, series, and grade, and personal information voluntarily submitted by the employee.

Authority for maintenance of the system:

5 CFR 335.102(a).

Purpose(s):

The records in this system are part of a Merit Promotion and Reassignment Program and consist of potential selectees for positions covered by the program. Records are maintained to allow selecting officials to make valid selections, as well as to provide a record of application requests for consideration. Also, records in the system are maintained as a means to track transfers allowed in the JOBX program. The JOBX program supports the Job Swap program by facilitating the non-competitive swap of employees between two duty stations, provided

have the same title, series, and grade. The Job Swap Program allows employees of encumbered positions to apply for and receive changes in geological locations without a need for vacancies to occur or new positions to be established.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A. To the Office of Personnel Management to enable the agency to make determination required by 5 CFR 335.103.

B. In a proceeding before a court or adjudicative body before which INS or the Department of Justice (DOJ) is authorized to appear when any of the following is a party to litigation or interest in litigation and such records are determined by INS or DOJ to be arguably relevant to the litigation: (1) The DOJ, or any DOJ component or subdivision thereof; (2) any DOJ employee in his or her official capacity; (3) any DOJ employee in his or her individual capacity when the DOJ has agreed to represent the employee; and (4) the United States where the DOJ determines that the litigation is likely to affect it or any of its subdivisions.

C. To the Merit Systems Protection Board or the Office of the Special Counsel in connection with appeals, special studies of the civil service and other merit systems, review of office of personnel rules and regulations, investigations of alleged or possible prohibited personnel practices, and other functions, e.g., as prescribed in 5 U.S.C. Chapter 12, or as may be authorized by law.

D. To the Equal Employment Opportunity Commission, when requested, in connection with investigations into alleged or possible discrimination practices in the Federal sector, examination of Federal affirmative employment programs, compliance by Federal agencies with the Uniform Guidelines on Employee Selection Procedures, or other functions vested in the Commission.

E. To a Member of Congress, or staff acting upon the Member's behalf, when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record.

F. To General Services Administration and National Archives and Records Administration for records management inspections conducted under the authority of 44 U.S.C. 2904 and 2905.

G. To the Federal Labor Relations Authority or its General Counsel when requested in connection with a representation case.

connection with investigations of allegations of unfair labor practices or matters before the Federal Service Impasses Panel.

H. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system's records.

I. To disclose information to an arbitrator to resolve disputes under a negotiated grievance procedure or to officials of labor organizations recognized under 5 U.S.C. Chapter 71 who have relevant and necessary to their duties of exclusive representation.

J. To the Union when required by contract as part of the processing of a grievance and/or arbitrator in the arbitration of a grievance.

K. Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information is stored on computer tapes, magnetic disks, and in file cabinets.

Retrievability:

Records may be retrieved by name, Social Security Number (SSN), or unique JOBX number.

Safeguards:

Most INS offices are located in buildings under security guard, and access to premises is restricted.

official identification. Offices are locked during non-duty hours. Access to this system is obtained through remote terminals that require the use of restricted passwords and a user ID. Paper records will be maintained in locked file cabinets. The JOBX server will be maintained in a secure computer facility.

Retention and disposal:

Records are retained in accordance with General Records Schedule 1, items 4, 15, 23(a), and 33b.

System manager(s) and address:

Director, National Hiring Center, Room 400, Whipple Federal Building, One Federal Drive, Minneapolis, MN 55111.

Notification procedure:

Inquiries should be addressed to the system manager.

Record access procedure:

Requests for access to a record from this system shall be in writing (e.g., cc: Mail can be used internally). If a request for access is made by mail the envelope and letter shall be marked "Privacy Act Request." The requester shall also provide a return address for transmitting the records to be released. The requester shall include his or her full name and SSN. An applicant can access his or her own record by logging onto the system using his or her own SSN and password. This brings the applicant to the main menu screen. The applicant can select, "View Application." The form is printable. The applicant can also move among the screens. Authorized selecting officials and coordinators can access records within their budget location code; and system administrators can access all records in the system.

Contesting record procedure:

Direct all requests to contest or amend information to the system manager noted above. Clearly and concisely state the information being contested, the reason for contesting it, and the proposed amendment thereof. Depending on the information, the coordinator or administrator will be able to make the correction. If the inaccurate information is from the National Fin

Center records, the applicant should contact his or her servicing administrative center a report the erroneous information. Clearly mark the envelope "Privacy Act Amendment Request." The record must be identified in the same manner as described for making a for access.

Record source categories:

Information contained in this system or records is obtained from the individuals covered system, or derived from information the individual supplied and from the National Financial Center database.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/INS-999

System name:

INS Appendix: List of principal offices of the Immigration and Naturalization Service.

Headquarters:

Immigration and Naturalization Service, 425 "I" Street NW., Washington, DC 20536.

Regional Offices:

Eastern Regional Office, 70 Kimball Avenue, South Burlington, VT 05403-6813.

Central Regional Office, 7701 North Stemmons Freeway, Dallas, TX 75247-9998.

Western Regional Office, PO Box 30080, Laguna Niguel, CA 92607-0080.

Administrative Centers:

Eastern Administrative Center, 70 Kimball Avenue, South Burlington, VT 05403–6813.

Southern Administrative Center, 1460 Prudential Drive, Dallas, TX 75235.

Northern Administrative Center, Bishop Henry Whipple Federal Building, Room 480, On Federal Drive, Fort Snelling, MN 55111–4007.

Western Administrative Center, 24000 Avila Road, Laguna Niguel, CA 92677–8080.

Border Patrol Academy:

DOJ/INS (FLETC) Artesia, 1300 West Richey Avenue, Artesia, NM 88210.

Officer Development and Training Facility, Building 64 FLETC, Glynco, GA 31524.

[\[TOP\]](#)

INTERPOL–United States National Central Bureau

JUSTICE/INTERPOL–001

System name:

The INTERPOL–United States National Central Bureau (USNCB) Records System, JUSTICE/INTERPOL–001.

System location:

INTERPOL–U.S. National Central Bureau, Department of Justice, Washington, DC 2053

Categories of individuals covered by the system:

Fugitives; wanted persons; criminal and non-criminal individuals who have been charge convicted or are subjects of a criminal investigation with international aspects; individual may be associated with stolen weapons, motor vehicles, artifacts, or similar items involv crime; victims related to humanitarian or criminal investigations; witnesses or confidentia

sources in a criminal investigation with international aspects; missing and/or abducted persons (including alleged abductors or other individuals associated with a missing or abducted person), and persons who are unable or unwilling to identify themselves; INTERPOL–US government and non-government contractor, judicial or law enforcement personnel engaged in the performance of official duties; applicants for a license, grant, contract or benefit; and applicants for positions with entities performing law enforcement and non-law enforcement functions.

Categories of records in the system:

The program records of the INTERPOL–USNCB consist of criminal and non-criminal cases which support the law enforcement and humanitarian functions performed by INTERPOL–USNCB. The files contain electronic data and hard copy records of facsimiles, fingerprints, photographs, criminal investigative reports, applicant checks related to law enforcement and non-law enforcement employment, security, and regulatory matters, licenses, grants, contracts, or benefits, and related data, radio messages (international), log sheets, notices, bulletins or posters, lookouts (temporary and permanent notices including identification information on an individual or item of interest to law enforcement authorities), investigative notes, computer printouts, letters, memoranda, witness statements and records related to deceased persons. Information about individuals includes names, aliases, places and dates of birth, addresses, physical descriptions, various identification numbers, reason for the request for lookouts, and details and circumstances surrounding the actual or suspected violation of law. Information about humanitarian requests or administrative/operational matters.

Authority for maintenance of the system:

22 U.S.C. 263a, and 28 CFR 0.34

Purpose(s):

The system manages data on foreign and domestic criminal and non-criminal, humanitarian and related law enforcement matters. These records are maintained to assist and support international law enforcement cooperation. The data includes fingerprints, photographs, criminal investigative reports, applicant checks, licenses, facsimiles, letters, memoranda, bulletins, posters, log sheets, notices, investigative notes, computer printouts, and similar. The data is used to facilitate the sharing of information between federal, state, local, and foreign law enforcement-related authorities in the United States, and foreign authorities engaged in

law enforcement functions including: the investigation of crimes and criminal activities, obtaining evidence, the sharing of law enforcement techniques, prevention of crime, assistance in humanitarian matters, the location and arrest of fugitives and wanted persons, the location of missing persons, border and immigration control, assistance in litigation, the sharing of history and background information used for investigative purposes, determinations regarding the suitability of applicants for law enforcement and non law enforcement-related employment and the issuance of a license, grant, contract, or benefit.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information may be disclosed as follows:

(1) In the event a record in this system of records, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, the relevant record may be referred, to the appropriate law enforcement and justice agencies whether foreign, federal, state, local or tribal, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.

(2) To any person or entity, and to the public generally, to the extent necessary to obtain information or cooperation in efforts to locate, identify, or arrest, if appropriate, fugitives, persons, missing persons, abducted persons, and persons who are unable or unwilling to identify themselves.

(3) To any entity maintaining civil, criminal or other information when necessary to obtain information relevant to a decision by a foreign, federal, state, local, or tribal agency concerning the hiring, appointment, or retention of an employee; the issuance or retention of a security clearance; the execution of a security or suitability investigation; the classification of a job; or the issuance of a contract, grant, license, or benefit.

(4) To officials and employees of a federal agency or entity, including the White House, when it has a need for information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance or retention of a security clearance; the execution of a security or suitability investigation; the classification of a job; or the issuance of a contract, grant, or benefit.

(5) In an appropriate proceeding before a court or administrative or regulatory body where

records are determined by the Department of Justice to be arguably relevant to the proceeding.

(6) To such recipients under such circumstances and procedures as are mandated by statute or executive agreement, or where disclosure is pursuant to an international treaty convention entered into and ratified by the United States.

(7) To the International Criminal Police Organization (INTERPOL) General Secretariat and National Central Bureaus in member countries; and to the INTERPOL Supervisory Board, an international board comprised of three judges having oversight responsibilities regarding the purpose and scope of personal information maintained in the international archives of INTERPOL.

(8) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

(9) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(10) To a Member of Congress or the Member's staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

(11) To the National Archives and Records Administration and General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(12) To foreign, federal, state, local and tribal licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

(13) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

(14) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(15) A record relating to a case or matter that has been referred by an agency, or that is a case or matter within the jurisdiction of an agency, or where the agency or its officials are affected by a case or matter, may be disseminated to such agency to notify the agency of the status of the case or matter or of any decision or determination that has been made, or for such other inquiries and reports as are necessary during the processing of the case or matter.

(16) To a foreign country, through the United States Department of State or directly to the representative of such country, to the extent necessary to assist such country in apprehending and/or returning a fugitive to a jurisdiction which seeks his return, or to assist such country in civil or criminal proceedings in which the United States or one of its officers or agencies has an interest.

(17) A record relating to a person held in custody pending or during arraignment, trial, sentencing, or extradition proceedings, or after conviction or after extradition proceedings, may be disseminated to a federal, state, local, or foreign prison, probation, parole, or pardon authority, or to any other agency or individual concerned with the maintenance, transportation, or release of such a person.

(18) To a federal, state, local, foreign, or international law enforcement agency to assist in general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency.

(19) To any entity or person where there is reason to believe that the recipient is or could become the target of a particular criminal activity or conspiracy, to the extent the information is relevant to the protection of life or property.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information is stored in file folders and in electronic word files at the INTERPOL–USNCB and the Washington Federal Records Center. Certain limited data, e.g., that which concerns fugitives and wanted, missing or abducted persons is stored in the Treasury Enforcement Communications System (TECS) TREASURY/CS 00.244, a system published by the U. S. Department of Treasury, and in the National Criminal Information Center (NCIC) [JUSTICE/001], for a limited time period, or until apprehended or located.

Retrievability:

Information is retrieved primarily by name, system identification number, personal identification number, and by weapon serial number or motor vehicle identification number.

Safeguards:

Information is safeguarded and protected in accordance with Department rules and procedures governing the handling of computerized information. Only those individuals specifically authorized have access to the INTERPOL–USNCB records. Access to INTERPOL–USNCB records is given only to those individuals who require access to perform official duties. In addition, USNCB information resides in the secured INTERPOL–USNCB offices which are staffed twenty-four hours a day, seven days a week. Automated data is password secured.

Retention and disposal:

Case files closed as of April 5, 1982 and thereafter are disposed of as follows: The hard copy (paper record) will be retained on site at the INTERPOL–USNCB for two years after closing the case. At the end of the two years post closing, the hard copy will be transferred to the Washington National Records Center for storage. The hard copy (paper record) of the case file may be destroyed five years after transfer to the Washington National Records Center, for a total of seven years post closing, if there has been no case activity. Information contained in electronic case files will be stored on a compact disc two years after closing the case and sent to the Washington National Records Center for destruction in five years, or seven years after closing the case, if there has been no case activity. Automated information will be flagged as an archived case and maintained on the LAN server for an indefinite period of time.

System manager(s) and address:

Chief, INTERPOL-United States National Central Bureau, Department of Justice, Washington, DC 20530.

Records Management Officer, INTERPOL-United States National Central Bureau, Department of Justice, Washington, DC 20530.

Information Resources Manager, INTERPOL-United States National Central Bureau, Department of Justice, Washington, DC 20530.

Notification procedure:

Inquiries regarding whether the system contains a record pertaining to an individual may be addressed to the Chief, INTERPOL-United States National Central Bureau, Department of Justice, Washington, DC 20530, or to the Freedom of Information Act (FOIA) Specialist at the same location. To enable INTERPOL-USNCB personnel to determine whether the system contains a record relating to him or her, the requester must submit a written request identifying the record system, identifying the category and type of records sought, and providing the individual's full name and at least two items of secondary information (date of birth, social security number, employee identification number, or similar identifying information).

Record access procedures:

The Attorney General has exempted the INTERPOL-USNCB system from the access, correction, and amendment provisions of the Privacy Act. Some records may be available under the Freedom of Information Act. Inquiries should be addressed to the FOIA/PA Officer, INTERPOL-United States National Central Bureau, Department of Justice, Washington, DC 20530. The request letter should be clearly marked "Freedom of Information Request" and a return address should be provided for transmitting any information to the requester.

Contesting record procedures:

See "Access procedures" above.

Record source categories:

Sources of information contained in this system include investigating reports, notes,

correspondence, messages, photographs, fingerprints, and other identification material; federal, state, local, tribal and foreign law enforcement and non-law enforcement agencies (including investigating reports from a system of records published by Department of Treasury Enforcement Communications System (TECS) TREASURY/CS 00.244 or the National Criminal Information Center (NCIC); other non-Department of Justice investigative agencies; client agencies of the Department of Justice); statements of witnesses and parties; and the work product of the staff of the INTERPOL–USNCB working on particular cases. Although the organization uses the name INTERPOL–USNCB for purposes of public recognition, the INTERPOL–USNCB is not synonymous with the International Criminal Police Organization (ICPO–INTERPOL), which is a private, intergovernmental organization headquartered in France. The Department of Justice USNCB serves as the United States liaison with the INTERPOL General Secretariat and works in cooperation with the National Central Bureau of other member countries, but is not an agent, legal representative, nor organization subordinate to the International Criminal Police Organization. The records maintained by the INTERPOL–USNCB are separate and distinct from records maintained by INTERPOL and the Department of Justice. The INTERPOL–USNCB does not have custody of, access to, nor control over the records of the International Criminal Police Organization.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(2), and (3), (e)(4)(G) and (H), (e)(5) and (8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2), and (k)(2) and (k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register*. See 28 CFR 16.103.

[\[TOP\]](#)

Justice Management Division

JUSTICE/JMD–002

System name:

Controlled Substances Act Nonpublic Records.

System location:

U.S. Department of Justice, Justice Management Division, Information Management and Security Staff, Washington, DC 20530.

Categories of individuals covered by the system:

Persons found guilty for the first time of violating section 404 of the Controlled Substances Act (21 U.S.C. 844), i.e., persons who knowingly or intentionally possessed a controlled substance, except as authorized by the Act, whose cases have been in subject of a disposition under 18 U.S.C. 3607(a) or an order of expungement under 18 U.S.C. 3607(c).

Categories of records in the system:

Arrest records of law enforcement agencies, which include personal data, photographs, fingerprints, copies of court orders and Form OBD-140 (18 U.S.C. 3607).

Authority for maintenance of the system:

This system is established and maintained in accordance with Public Law 98-473, Chapter 2, the Sentencing Reform Act of 1984 (18 U.S.C. 3607).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records are retained by the Department of Justice and are available only to a Federal court upon that court's issuance of an order demanding such records solely for the purpose by said court in determining whether or not a person found guilty of an offense under section 404 of the Controlled Substances Act (21 U.S.C. 844) qualifies for the disposition provided in 18 U.S.C. 3607(a) or the expungement provided in 18 U.S.C. 3607(c).

Release of information to the National Archives and Records Administration:

Subject to approval by the Attorney General or the President under 44 U.S.C. 2906, a record from this system of records may be disclosed to the National Archives and Records Administration (NARA) as part of a records management inspection conducted under the authority of 44 U.S.C. 2904.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Records are stored in a locked room.

Retrievability:

Records are indexed by the name of the offender.

Safeguards:

Access to these records is restricted to the Departmental Records Officer and Assistant Director, Information Security and Records Management, information Management and Security Staff, Justice Management Division.

Retention and disposal:

Records are retained in accordance with records retention and disposal schedules approved by the Archivist of the United States.

System manager(s) and address:

Director, Information Management and Security Staff, Justice Management Division, U.S. Department of Justice, Washington, DC 20530.

Notification procedure:

Same as the System Manager.

Record access procedures:

Same as the System Manager.

Contesting record procedures:

Same as the system manager.

Record source categories:

Law enforcement agencies and Federal courts.

Exemptions claimed for the system:

The Attorney General has exempted the system from subsection (d) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(c) and (e) and have been published in the *Federal Register*. The proposed rule which update the justification for the exemption is being published in today's *Federal Register*.

[\[TOP\]](#)

Justice/JMD-003

System name:

Department of Justice Payroll System, Justice/JMD-003.

System location:

This system of records is managed by the Department of Justice (DOJ), Justice Management Division (JMD), Director, Personnel Staff, Washington, DC 20530. DOJ has contracted with the Department of Agriculture's National Finance Center (NFC) in New Orleans, Louisiana, to maintain payroll information and conduct payroll-related activities for its employees. Conversion to the NFC began in July of 1991 and was incrementally completed as of March 1993. Payroll records in electronic or paper format may be found in the following locations:

a. Post-Conversion Records: On a computer maintained by the NFC in New Orleans, Louisiana; and at backup facilities in Philadelphia, Pennsylvania. Relevant data may also be stored on Justice Data Center computers or servers at the DOJ for use in distributing personnel and accounting information to the individual DOJ Bureaus and components. Paper and electronic payroll information may be kept at various time and attendance recording and processing stations around the world. Paper records may be located in the DOJ's Personnel

Staff, Washington, DC 20530, in servicing personnel offices throughout the DOJ, and in offices of employee supervisors and managers.

b. Pre-Conversion Historical Records: On magnetic tape at the Justice Data Center in Rockville, Maryland 20854; on microfiche maintained by the DOJ Finance Staff; and in print format maintained by the DOJ's Finance and Personnel Staffs, servicing personnel offices of employee supervisors and managers.

Categories of individuals covered by the system:

Current and former DOJ employees.

Categories of records in the system:

Any and all records essential to the conduct of payroll-related activities. Included may be

- Personal identifying/personnel data;
- Time and attendance records;
- Leave records;
- Allotment or deduction information such as bonds, garnishments, health benefits, life insurance, Thrift Savings Plan (TSP), and other savings, retirement, and union dues;
- Travel and relocation information;
- Court orders to initiate garnishments;
- Check mailing and Direct Deposit / Electronic Funds Transfer information;
- Tax, withholding, and exemption information;
- Accounting and organization funding information;
- Salary, severance pay, award, and bonus information; active retirement records;

- Former employee pay records;
- Employee death records;
- Returned employee check and canceled salary payment records;
- Indebtedness records, e.g., overpayment of pay or travel.

Authority for maintenance of the system:

5 U.S.C. 301, 5516, 5517, 5520; 26 U.S.C. 6011, 6109; 44 U.S.C. 3101.

Purpose(s):

This system of records is maintained to enable the DOJ to administer the payroll and pay related functions, and any other related financial matters, in accordance with applicable laws, rules, and regulations and the requirements of the General Accounting Office (GAO), the Office of Personnel Management (OPM), and the Federal Retirement Thrift Investment Board (FRTIB). The system enables the DOJ to prepare and document payment to all DOJ employees entitled to be paid and to effect all authorized deductions from gross pay; to coordinate pay, leave and allocation of funds with personnel functions and other related activities; meet internal and external reporting requirements; support investigations of fraud, the collection of debts, and litigation activities.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Pursuant to subsection (b)(3) of the Privacy Act, the DOJ may disclose relevant and non-exempt data as follows:

In accordance with an interagency agreement, as provided for in Office of Management and Budget (OMB) implementing guidelines (40 FR 28948), the DOJ may disclose records to the U.S. Department of Agriculture (USDA), National Finance Center (NFC), in order to effect financial transactions on behalf of the DOJ related to employee pay.

Specifically, the NFC may effect employee pay or deposit funds on behalf of DOJ employees.

and/or it may withhold, collect or offset funds from employee salaries as required by law necessary to correct overpayment or amounts due. For example, the NFC will routinely the necessary disclosures to the Treasury Department for the issuance of payments; to Federal, State, and local authorities and the Social Security Administration for tax withholdings; to OPM for retirement contributions; and, according to employee directions, to the appropriate financial institutions, charitable organizations, unions, health carriers, or other appropriate entities to effect such pay distributions as savings bonds, charitable contributions, alimony, child support, union dues, health and life insurance, and TSP contributions. In addition, the NFC will use the data to perform related administrative activities such as to process payroll vouchers chargeable to DOJ funds; and either to perform or participate in routine audit/oversight operations of USDA/DOJ management and/or of GAO, OMB, OPM, and and to meet related reporting requirements.

In addition, where determined to be appropriate or necessary, the DOJ may disclose records from this system as follows; or, DOJ may authorize the NFC to make the disclosures:

- A. To Federal, State, or local housing authorities to enable these authorities to determine eligibility for low cost housing.
- B. To heirs, executors and legal representatives of beneficiaries for estate settlement purposes.
- C. To State and local courts of competent jurisdiction for the enforcement of child support, alimony, or both, pursuant to 42 U.S.C. 659.
- D. To individuals, organizations, or agencies to enable such person, organization, or agency to determine the identity or location of a current or former Federal employee to collect debts owed, where collection of such debts are authorized (either by statute, implementing regulation, or order issued pursuant thereto) and the individual, organization, or agency provided sufficient evidence as will reasonably validate such claims, e.g., where a spouse or creditor seeking to obtain a garnishment of wages for such purposes as alimony and/or child support has provided a court order to substantiate the indebtedness. Information relevant to the request for such garnishment may include informing the individual, organization, or agency of the unavailability of funds where, for example, a currently active garnishment precludes implementation of a further garnishment.
- E. To the Office of Child Support Enforcement (OCSE), Administration for Children and Families, Department of Health and Human Services, any information specifically required by the OCSE.

statute or implementing regulation or otherwise determined to be necessary and proper OCSE's use (as outlined more specifically in relevant OCSE published Privacy Act system records) in locating individuals owing child support obligations, and in establishing and collecting child support obligations from such individuals, including enforcement action. Information disclosed may include: name, address, date of birth, date of hire, duty station, social security number of the employee; the wages paid to the employee during the pre quarter; and the appropriate address and Federal Employer Identification Number of the Department of Justice.

F. To the appropriate Federal, State, or local agencies, e.g., to state unemployment agencies and/or the Department of Labor, to assist these agencies in performing their lawful responsibilities in connection with administering unemployment, workers' compensation and other benefit programs; and similarly, to such agencies to obtain information that may aid the Department of Justice in performing its lawful responsibilities as they relate to such programs.

G. To appropriate agencies, entities, and persons when (1) The Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize or remedy such harm.

H. Where a record, either on its face or in conjunction with other information indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, foreign, or tribal, law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.

I. To the Internal Revenue Service (IRS) to obtain taxpayer mailing addresses for the purpose of locating such taxpayer to collect or compromise a Federal claim against the taxpayer.

J. To a person or organization with whom the head of the agency has contracted for collection services to recover indebtedness owed to the United States. Addresses of taxpayers obtained

from the IRS will also be disclosed, but only where necessary to locate such taxpayer to or compromise a Federal claim.

K. To a Federal, State, local, or foreign agency or to an individual or organization if there is reason to believe that such agency, individual, or organization possesses information relating to the debt, the identity or location of the debtor, the debtor's ability to pay, or relating to any other matter which is relevant and necessary to the settlement, effective litigation and enforcement of collection of the debt, or relating to the civil action trial or hearing, and the disclosure is reasonably necessary to elicit such information or to obtain the cooperation of a witness or the agency.

L. To employers to effect salary or administrative offsets to satisfy a debt owed the United States by that person; or when other collection efforts have failed, to the IRS to effect an offset against an income tax refund otherwise due.

M. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

N. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, an individual who is the subject of the record.

O. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

P. In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator holds the records to be relevant to the proceeding.

Q. To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion on such matters as settlement, plea bargaining, or informal discovery proceedings.

R. To contractors, grantees, experts, consultants, students, and others performing or working

on a contract, service, grant, cooperative agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system of records.

S. To a former employee of the Department for purposes of: responding to an official inquiry of a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Consistent with the foregoing routine use provisions, the Department may disclose records from this system of records for use in a computer matching program (as defined in the Privacy Act, 5 U.S.C. 552a (a)(8)). In accordance with the requirements of the Privacy Act, the Department will be given advance notice in the *Federal Register* of the Department's participation in such computer matching program(s).

In addition to the above routine use disclosures under subsection (b)(3) of the Privacy Act, DOJ may make relevant and necessary disclosures as permitted by other Privacy Act disclosure provisions.

Finally, 31 U.S.C. 3711 requires that the notice required by the Privacy Act at 5 U.S.C. 552a (e)(4) must indicate that information in the system may be disclosed to a consumer reporting agency pursuant to subsection (b)(12). Such notice is provided as follows:

Notice of Disclosure to Consumer Reporting Agencies Under Subsection (b)(12) of the Privacy Act: Records relating to the identity of debtors and the history of claims may be disseminated to consumer reporting agencies to encourage payment of the past-due debt. Such disclosure will be made only when a claim is overdue and only after due process steps have been taken to notify the debtor and give him or her a chance to meet the terms of the debt.

(Any disclosures that may be made for debt collection purposes, whether made pursuant to subsection (b)(3) or (b)(12) of the Privacy Act, would be made only when all the relevant process or procedural steps established by the relevant statutes and implementing regulations have been taken.)

Policies and practices for storing, retrieving, accessing, Retaining and Disposing of

in the system:***Storage:***

Records are stored on disks, magnetic tapes, microfiche, paper, and direct access storage device (DASD).

Retrievability:

Records are retrieved by name or social security number.

Safeguards:

Access to premises where records are stored is restricted via building passes and security guards. Access to all records is supervised and restricted to those employees with a need to know. In addition, access to computerized records is protected by encryption, password protection, and appropriate user ID's. Access to terminals is limited to persons with terminal identification numbers. These numbers are issued only to employees who have a need to know in order to perform job functions relating to personnel and payroll matters.

Retention and disposal:

Records are disposed of in accordance with General Records Schedule No. 2 issued by the National Archives and Records Administration.

System manager(s) and address:

Director, Personnel Staff, Justice Management Division, Department of Justice, National Personnel Building, Room 1110, 1331 Pennsylvania Avenue, NW., Washington, DC 20530.

Notification procedure:

The individual may address inquiries to the servicing personnel office of the Department component(s) by which he/she is or was employed. Address of Department component(s) may be found in Appendix I, to part 16 of 28 Code of Federal Regulations. Updated listings are available on the DOJ Web site on the Internet (<http://www.usdoj.gov/>). The individual may address his/her request to the System Manager named above.

Record Access Procedure:

A request for access to a record must be made in writing to the System Manager named with the envelope and letter clearly marked "Privacy Act Access Request." The request include a general description of the records sought. Include in the request the full name requester, his or her current address, and date and place of birth, with notarized signed dated signature submitted under penalty of perjury (28 CFR 16.41(d)).

Contesting record Procedure:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Record Access procedures listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information is not subject to amendment, including tax return information.

Record source categories:

Individuals covered by the system; agency records; financial institutions or employee organizations; previous Federal employers; consumer reporting agencies; debt collection agencies; and the courts.

Exemptions Claimed for the System:

None.

[\[TOP\]](#)

JUSTICE/JMD-005

System name: Grievance Records.

System location:

Records relating to grievances originating in an office, board or division (defined in 28 C.F.R. 16.41(d)) except for the Executive Office for United States Attorneys, are located in the Office of the Assistant Director for Personnel Service. Records relating to grievances originating in the

Executive Office for United States Attorneys or in a United States Attorney's office are located in the office of the Personnel Officer, Executive Office for United States Attorneys. Records relating to grievances originating in a particular bureau (defined in 28 CFR 0.1) are located in the central personnel office of the bureau where the grievance originated, except for the Federal Bureau of Investigation (FBI) which is excluded from coverage of the Agency Administrative Grievance System by 5 CFR 771.206(a). (See caption "System managers' addresses.")

Categories of individuals covered by the system:

Current or former Department of Justice employees, except for employees of the FBI, who have submitted grievances in accordance with 5 CFR part 771 (Office of Personnel Management (OPM) regulations) and the Department's grievance procedures, or in accordance with a negotiated grievance procedure.

Categories of records in the system:

The system contains records relating to grievances filed by the agency employees under 5 CFR part 771 and the Department's grievance procedures, or under a negotiated grievance procedure. These case files contain all documents related to the grievance, including statements of witnesses, reports of interviews and hearings, examiner's findings and recommendations, or arbitration award, and a copy of any original and final decision and related correspondence and exhibits.

Authority for maintenance of the system:

5 U.S.C. 552a(f); 5 CFR part 771; 5 U.S.C. 1032, 3301, 3302; E.O. 10577; 3 CFR 1954-Comp., p. 218.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records and information in these records may be used:

- a. To disclose pertinent information to another appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the Department becomes aware of an indication of a violation

potential violation of civil or criminal law or regulation.

b. To disclose information to any source from which additional information is requested course of processing a grievance to the extent necessary to identify the individual, inform source of the purpose(s) of the request, and identify the type of information requested.

c. To disclose information to another Federal agency (in response to its request) for its use in the hiring or retention of an employee, the issuance of a security clearance, the conducting of a security and/or suitability investigation of an individual, the classifying of jobs, the letting of a contract, or the issuance of a license, grant, or other benefit to the extent that the information is relevant and necessary to its decision on the matter.

d. To provide information to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

e. To disclose information to another Federal agency or to a court when the Government is a party to a judicial proceeding before the court.

f. By the National Archives and Records Administration and the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2908.

g. By the Department or OPM in the production of summary descriptive statistics, if available, and analytical studies in support of the function for which the records are collected and maintained, or for related work force studies. While published statistics and studies do not contain individual identifiers, in some instances the selection of data elements included in a study may be structured in such a way as to make the data individually identifiable by inference.

h. To disclose information to officials of the Merit Systems Protection Board; the Special Counsel; the Federal Labor Relations Authority and its General Counsel; the Equal Employment Opportunity Commission; or, the OPM when requested to perform their authorized duties.

i. To disclose in response to a request for discovery or for appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding.

j. To provide information to labor organization officials recognized under the Civil Service Reform Act when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting work conditions.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

These records are maintained in file folders.

Retrievability:

These records are retrieved by the names of the individuals on whom they are maintained.

Safeguards:

These records are maintained in lockable metal filing cabinets to which only authorized personnel have access.

Retention and disposal:

These records are disposed of three years after closing of the case. Disposal is by shredding or burning.

System manager(s) and address:

a. Offices, Boards and Divisions, Assistant Director for Personnel Service, U.S. Department of Justice, 633 Indiana Avenue, NW, Washington, DC 20530.

b. Bureau of Prisons, Personnel Director, Bureau of Prisons, HOLC Building, 320 First Street, NW, Washington, DC 20534.

c. Drug Enforcement Administration, Deputy Assistant Administrator for Personnel, Drug Enforcement Administration, 1405 I Street, NW, Washington, DC 20537.

d. Immigration and Naturalization Service, Assistant Commissioner for Personnel and Training, Immigration and Naturalization Service, CAB Building, 425 I Street, NW, Washington, DC 20530.

e. Office of Justice Programs, Director, Office of Personnel, Office of Justice Programs, Indiana Avenue, NW, Washington, DC 20530.

f. United States Marshals Service, Personnel Officer, U.S. Marshals Service, 600 Army-Navy Building, Arlington, VA 22202.

g. Executive Officer for United States Attorneys, Personnel Officer, 601 D Street, NW, P. O. Box 1000, Henry Building, Washington, DC 20530.

Notification procedure:

Individuals who have filed grievances may contact the appropriate personnel office (named under the caption "System managers" and addresses" above) where the action was processed regarding the existence of such records on them. They must furnish the following information for the records to be located and identified:

- a. Name.
- b. Approximate date of closing of the case and the subject matter of the grievance.
- c. Organization component involved.

Record access procedures:

Individuals who have filed grievances may request access to the official copy of the grievance file by contacting the appropriate personnel office (named under the caption "System

managers and addresses" above) where the action was processed. Individuals must provide the information listed under the caption "Notification procedures" for their records to be located and identified. Individuals requesting access must also follow the Department's Privacy regulations (28 CFR 16.41) regarding access to records and verification of identity.

Contesting record procedures:

Review of requests from individuals seeking amendment of their records which have been the subject of a judicial or quasi-judicial action will be limited in scope. Review of amendment requests of these records will be restricted to determining if the record accurately documents the action of the agency ruling on the case and will not include a review of the merits of the action, determination, or finding.

Individuals wishing to request amendment to the records to correct factual errors should contact the personnel office (named under the caption "System managers and addresses" above) where the grievance was processed. Individuals must furnish the information listed under the caption "Notification procedures" for their records to be located and identified.

Individuals requesting amendment must also follow the office's Privacy Act regulations (28 CFR 16.41) regarding amendment to records and verifications of identity.

Record source categories:

Information in this system of records is provided:

- a. By the individual on whom the record is maintained.
- b. By testimony of witnesses.
- c. By Department officials.
- d. From related correspondence from organizations or persons.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/JMD-006

System name: Debt Collection Management System, JUSTICE/JMD-006

System location:

Department of Justice, Justice Management Division (JMD), Central Intake Facility (CIF), Bonifant Street, Suite 220, Silver Spring, Maryland.

Categories of individuals covered by the system:

Persons indebted to the United States who have allowed their debts to become delinquent whose debts have been sent by client Federal agencies to the Department of Justice for settlement or enforced collection through litigation.

Categories of records in the system:

This system of records contains records for all 94 judicial districts of the United States. It contains records relating to the negotiation, compromise, settlement, and litigation of debts owed the United States. Records will consist of an automated support data base and temporary custody of case files. Case files are assigned promptly to a U.S. Attorney (USA) where the Department has contracted for their services, to private counsel to undertake enforced debt collection action.¹ This system describes case files during the period when they are in the possession of the JMD, CIF. Upon assignment of a case file to a USA or to private counsel, the case is covered by the Debt Collection Enforcement System, JUSTICE/USA-015.¹

Private counsel are employed under a statutorily-authorized pilot program in specific judicial districts. Pub. L. 102-58 (November 10, 1992) authorized a four-year extension of the pilot program through September 30, 1996, and expanded the number of judicial districts from 15. Ten of these districts have been identified as: Central District of CA; Northern District of CA; Eastern District of NY; Southern District of FL; Eastern District of MI; Southern District of NY; District of Columbia; Middle District of FL; Western District of LA; and the District of NJ.

The client agency case file includes such documents as the Claims Collection Litigation

Report; Certificate of Indebtedness; any partial payment records, status reports, correspondence, and any other documentation developed during the negotiation of the

An automated data base provides litigation/administrative support to private counsel and in the pilot districts² and creates an inventory of cases assigned to the 94 judicial district data base contains data extracted from the case file and any data generated or developed to support the administrative operations of the debt collection program. Information may include personal data, e.g., name, social security number, date of birth, and locator information; claim information, e.g., type of claim such as benefit overpayment, loan default, bankruptcy, etc.; payment demand information, compromise offered, etc.; account information, e.g., debt payments including principal, penalties, interests, and balances, etc.; information regarding debtor's employment, ability to pay, property liens, etc.; value of claim, name of source which provided the loan or benefit; information on the status and disposition of cases at intervals of time; and any other information related to the negotiation, compromise, settlement or litigation of debts owed the United States, or to the administrative management of the collection program.

² The ultimate goal is to provide fully automated debt collection litigation support to all 94 USAs. While moving toward this goal, the Department envisions a system that will maintain summary level data for all 94 USAs until all districts can be provided, serially, full administrative and litigation support.

(When a case is closed or a judgment is obtained, the USAs in both pilot and non-pilot districts notify the CIF as to the final disposition of the case on a monthly basis.)

Authority for maintenance of the system:

31 U.S.C. 3711 and 3718, and 28 U.S.C. 3201

Purpose(s):

Title 31 U.S.C. 3711 authorizes the Attorney General to conduct litigation to collect delinquent debts due the United States; 31 U.S.C. 3718(b) authorizes the Attorney General to contract with private counsel to assist the Department (specifically, the USAs) in collecting consumer and commercial debts owed the United States on a pilot project basis; and Chapter 176 of Title 28, United States Code ("Federal Debt Collection Procedure"), authorizes the Attorney General to obtain both prejudgment and postjudgment remedies against delinquent debtors.

and section 3201(e) of that Chapter states that a judgment against such a debtor creates a lien on all real property of the debtor and renders that debtor "ineligible" for any grant or loan made, insured, financed or guaranteed by the Federal Government. Accordingly, this system of records is maintained by JMD under contract by means of the CIF to assist the Attorney General in conducting this debt litigation through the USAs in all 94 judicial districts (for an indefinite period) and, where appropriate, through contract private counsel under a pilot program (for periods specified by legislation). The CIF receives debt collection files from Federal agencies for assignment to private counsel in any selected pilot judicial districts where the Department has contracted for their services and/or to the USAs in all 94 judicial districts. The CIF furnishes automated litigation/administrative support to such counsel and to USAs in the pilot districts,⁴ and creates an inventory of all debts referred by USAs and by client agencies to the Department (and subsequently referred/assigned by the CIF to such counsel and to USAs in all 94 judicial districts) for enforced collection via litigation. The inventory enables the Department to provide statistical data to the Congress and the Office of Management and Budget on debt collection activities as required by 31 U.S.C. 3718(c).

³ A separate system of records entitled "Debt Collection Enforcement System, Justice/USA-015," covers the records as maintained by the USAs and such counsel, and identifies the relevant judicial districts.

⁴ See note 2, *supra*.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

In the course of its collection and enforcement activities, the Department may release client agency case files to the CIF to conduct the administrative operations of the debt collection program. Through the administrative operations of the CIF, the Department will release the case files and any related records or information created by the CIF to the contract private counsel to negotiate, settle, and litigate debts owned by the United States.

The Department may also disclose relevant records or information from this system as follows:

(a) To client agencies who have referred debt collection cases to the Department for settlement or litigation and enforced collection to notify such agencies of the status of the case or a decision or determination that has been made, or to make such other inquiries and reports

are necessary during the processing of the case.

(b) To a Federal agency in response to its request and in connection with hiring or reter an employee, the issuance of the required security clearance, the reporting of an invest of an employee, the letting of a contract, or the issuance of a license grant or other ben the requesting agency, to the extent that the information relates to the requesting agency decision on the matter.

(c) In a proceeding before a court or adjudicative body before which the Department or private counsel who are authorized to appear when any of the following is a party to litigation has an interest in litigation and such records are determined by the Department or contract private counsel to be arguably relevant to the litigation: (1) The Department, or any subdivision thereof, or contract private counsel, or (2) any employee of the Department or contract private counsel in his or her official capacity or (3) any employee of the Department or contract private counsel in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (4) the United States, where the Department or contract private counsel determines that the litigation is likely to affect the Department or any of its subdivisions.

(d) To volunteer student workers and students working under a college work-study program is necessary to enable them to perform their function;

(e) To employees or to contract personnel to access the records for Privacy Act training purposes.

(f) To (1) a Federal, state, local or foreign agency, an organization or individual to elicit information to assist the Department in the settlement or effective litigation and enforcement collection of the overdue debt; and (2) the Internal Revenue Service to obtain the mailing address of a taxpayer to collect or to compromise a debt owed by the taxpayer to the United States.

(g) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(h) To a Member of Congress or staff acting upon the Member's behalf when the Member

staff requests the information on behalf of and at the request of the individual who is the subject of the record.

(i) To the National Archives and Records Administration and to the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(k) To the Department of Housing and Urban Development (HUD) for its use in evaluating the credit worthiness of Federal loan applicants. Ultimately, this information may be accessible to other entities to determine credit worthiness; that is, HUD may permit access to its data (possibly through a computer matching program) by authorized employees of Federal agencies and private lenders (i.e., private lenders of Federally insured or guaranteed loans) to determine the credit worthiness of Federal loan applicants. Specifically, HUD operates an automated telephonic prescreening system (the Credit Alert Interactive Voice Response System) through which relevant information may be provided to assist such lenders and agencies in identifying whether there are any outstanding judgments against the applicant or other Federal debts, the amount of the debt, the status thereof, and any other information that may assist the lender/agency in making a decision on whether to approve or not approve an application for a loan. (See 28 U.S.C. 3201(e).)

Disclosure to consumer reporting agencies: Disclosure to consumer reporting agencies under subsection (b)(12) of the Privacy Act: Disclosure to consumer reporting agencies in accordance with section 3711(f) of Title 31 (as authorized under subsection (b)(12) of the Privacy Act): Relevant records may be disclosed to a consumer reporting agency as in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)) where such information is directly related to the identity of debtors and the history of claims contained in this system of records and for the purpose of encouraging repayment of overdue debts. Such disclosure may be made only when the debt is overdue and only after due process steps have been taken to notify the debtor and give him or her a chance to meet the terms of the debt. Addresses of taxpayers obtained by the Department of the Treasury may be disclosed to consumer reporting agencies only for the purpose of allowing such agencies to prepare a commercial credit report on the tax use by the Department. Prior to such disclosure, satisfactory assurances will be obtained from such consumer reporting agency concerning compliance by that agency with the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) and any other Federal law governing the provision of consumer credit information.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disclosing information in the system:

Storage:

Case files are stored in locked rooms; automated data is stored on magnetic tape.

Retrievability:

Data is retrieved by name of debtor.

Safeguards:

Access to records is restricted to those personnel who must have access to perform the function and is limited to those cases assigned. Case files are maintained separately in locked rooms during non-duty hours. Access to automated data requires the use of the proper password and user identification code.

Retention and disposal:

Paper records in this system will be returned to client Federal agencies for disposition; automated information will be erased ten years after the related case files reported in the Collection Enforcement System, JUSTICE/USA-015 have been closed.

System manager(s) and address:

Deputy Assistant Attorney General, Debt Collection Management, Justice Management Division, Department of Justice, Washington, DC 20530.

Notification procedure:

Address inquiries to Deputy Assistant Attorney General, Debt Collection Management, Management Division, Department of Justice, Washington, DC 20530.

Record access procedures:

Address requests for access to Deputy Assistant Attorney General, Debt Collection Management, Justice Management Division, Department of Justice, Washington, DC 20530. Clearly mark the envelope "Privacy Access Request." Include in the request the debtor's date of birth, address, and any other identifying information which may be of assistance locating the record, e.g., name of the case or Federal agency to whom the debtor is indebted. In addition, include notarized signature of the debtor as well as the name and address of individual to receive the information if other than the debtor.

Contesting records procedures:

Address requests to Deputy Assistant Attorney General, Debt Collection Management, Management Division, Department of Justice, Washington, DC 20530. State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment to the information.

Record source categories:

The individuals covered by the system; client agencies of the Department to whom the individual is indebted; an attorney or other representative for the debtor and/or payor; any Federal, State, local, foreign, private organization or individual who may have information relating to the debt, the debtor's ability to pay or any other information relevant and necessary to assist in the settlement or effective litigation and enforced collection of the debt.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/JMD-007

System name: Accounting System for the Offices, Boards and Divisions and the United States Marshals Service.

System location:

United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

All individuals on whom vouchers are submitted requesting payment for goods or services rendered (except payroll vouchers for Department of Justice employees,) including vendors, contractors, experts, witnesses, court reporters, travelers, and employees.

Categories of records in the system:

All vouchers processed, i.e., all documents required to reserve, obligate, process and effect collection or payment of funds. (Excluded from the system are payroll vouchers.)

Authority for maintenance of the system:

The system is established and maintained in accordance with 31 U.S.C. 3512.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

After processing the vouchers, the records are used to maintain individual financial accountability; to furnish statistical data (not identified by personal identifiers) to meet both internal and external audit and reporting requirements; and to provide Administrative Office of the Offices, Boards and Divisions and the United States Marshals Service with information on vouchers by name and social security number.

Release of information to the news media. Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from system of records maintained by the Department of Justice unless it is determined that release of the specified information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice not otherwise required to be released pursuant to 5 U.S.C. 552 may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at request of an individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed for a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Release of taxpayer mailing address information. Information contained in the system or records may be disclosed to the Internal Revenue Service (IRS) to obtain taxpayer mailing addresses for the purpose of locating such taxpayer to collect or compromise a Federal claim against the taxpayer.

Release of information to consumer reporting agencies. Information directly related to the identity of debtors and the history of claims contained in the system or records may be disclosed to consumer reporting agencies for the purpose of encouraging repayment of overdue debts. Such disclosures will be made only when a claim is overdue and only after process steps have been taken to notify the debtor and give him or her a chance to meet the terms of the debt. Addresses of taxpayers obtained from the Department of the Treasury will be disclosed to consumer reporting agencies only for the purpose of allowing such agencies to prepare a commercial credit report on the taxpayer for use by the Department.

Release of information about debtors. Information contained in the system of records may be disclosed in order to effect salary or administrative offsets to satisfy a debt owed the United States by that person. Such disclosures will be made only when all procedural steps established by the Debt Collection act have been taken.

Release of information to debt collection agencies. Information contained in the system or records may be disclosed to a person or organization with whom the head of the agency has contracted for collection services to recover indebtedness owed to the United States. Addresses of taxpayers obtained from the Department of the Treasury will also be disclosed but only where necessary to locate such taxpayer to collect or compromise a Federal claim.

Release of information to United States Attorneys. Information contained in the system's records may be disclosed to United States Attorneys' offices for litigation and enforced collection.

Release of information in a proceeding before a court or adjudicative body. Records with system or any facts derived therefrom, may be disseminated before a court or adjudicative body before which the Justice Management Division is authorized to appear when i. the Management Division, or any subdivision thereof, or ii. any employee of the Justice Management Division in his or her official capacity, or iii. any employee of the Justice Management Division in his or her individual capacity where the Department of Justice has agreed to represent the employee, or iv. the United States, where the Justice Management Division determines that the litigation is likely to affect it or any of its subdivisions, is a party to the litigation or has an interest in litigation and such records are determined by the Justice Management Division to be arguably relevant to the litigation.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Magnetic disks, magnetic tapes, microfilm, and file folders.

Retrievability:

Records on magnetic tapes and disks are primarily retrieved by social security number or digital identifiers. Records covering all fiscal years prior to Fiscal Year 1983 are maintained on paper form; as of Fiscal Year 1983 paper records have been converted to microfilm. Records on paper form and on microfilm are retrieved by batch and controlled by schedule on which

Safeguards:

Information contained in the system is unclassified. Operational access to information maintained on magnetic disks is controlled by the convention of the operating system. This is normally by password key. These passwords are issued only to employees who need to know in order to perform job functions relating to financial management and accountability. Records are also safeguarded in accordance with organizational rules and procedures. Access is limited to personnel of the Department of Justice who have a need for the records in the performance of their official duties.

Retention and disposal:

Magnetic disks, magnetic tapes, microfilm, and paper documents are retained for a period of six years and three months and subsequently destroyed in accordance with regulations prescribed by the General Accounting Office and promulgated by the General Services Administration.

System manager(s) and address:

Directors, Finance Staff, Office of the Comptroller, Justice Management Division, U.S. Department of Justice, 10th & Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Same as the System Manager.

Record access procedures:

Same as the System Manager.

Contesting record procedures:

Same as the System Manager.

Record source categories:

Submitted by operating accounting personnel or individual of record.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/JMD-009

System name:

Debt Collection Offset Payment System, Justice/JMD-009.

System location:

Department of Justice (DOJ), Justice Data Center, 1151D Seven Locks Road, Rockville,

Categories of individuals covered by the system:

Federal debtors. Federal debtors include (but may not be limited to) those who have received overpayments through direct financial assistance, those who owe debts of restitution based on civil or criminal judgments entered by Federal courts, and those who have obtained insured or guaranteed loans from Federal agencies, and (a) whose delinquent debts have been referred to client Federal agencies to the DOJ for enforced collection through litigation or (b) whose delinquent debts are owed directly to the DOJ.

Categories of records in the system:

Automated records include a data base on delinquent debts by debtor name, taxpayer name, and Taxpayer Identification Number (TIN), type of government claim involved, and the Federal agency entitled to notice of funds collected. (Such debts are referred by United States Attorneys (USAs) from client Federal agencies), and by other DOJ components). The data base also includes (1) information identifying those delinquent debtors who are present or former Federal employees, or members of the Armed Forces and whose salaries or other Federal benefit payments may be eligible for administrative offset by their respective employers (and whose debts may be referred to such agencies for such offsets), (2) voluntary payments made to the DOJ Jockbox, and (3) debt amounts offset by the Internal Revenue Service against income tax refunds. Manual records include computer-generated reports that list

delinquent debtors by name, TIN, tax year, and the USA or other DOJ component (and/or Federal agency) that referred the delinquent debt for collection, the referring agency's contact number, the status of the account, and the balance owed.

Authority for maintenance of the system:

Pub. L. 97-365, the Debt Collection Act of 1982; sec. 3 of Pub. L. 102-589, the Cash Management Improvement Act Amendments of 1992; and Pub. L. 104-134, the Debt Collection Improvement Act of 1996.

Purpose(s):

This system of records is used first to determine whether administrative offset of the delinquent debts can be made by Federal agencies against compensation due delinquent debtors who are present or former employees of such agencies, or present or former members of the Armed Forces. Second, it is used to refer delinquent debts to the IRS for offset against any income tax refunds that may be due the debtors under the IRS Federal Income Tax Refund Offset Program, to record data on any offsets made, and to maintain historical data on delinquent debtor payments through the Program.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

DOJ may disclose relevant information from this system as follows:

- (a) To the IRS to obtain the mailing address of a taxpayer for the purpose of locating such taxpayer to collect or to compromise a debt owed by the taxpayer to the United States.
- (b) To the Department of Defense (DOD) and United States Postal Service (USPS) to conduct computer matching programs to identify and locate debtors who receive Federal salaries and/or pension, annuity or other Federal benefit payments. Except where such debts are voluntarily repaid, the debts of those individuals who have been so identified will be returned to the DOJ component, or to the USA for referral to the appropriate Federal agency, for collection of administrative salary, or other procedure to offset Federal payments.
- (c) To the IRS to conduct computer matching programs to identify individuals entitled to tax refunds against which tax refund offsets would be appropriate and to enable the IRS to

the taxpayer's tax refund. (A tax refund offset may be initiated where the debt cannot be collected against the payment of Federal benefits such as Federal salaries, annuities, pensions, or other Federal payments.)

(d) These records pertaining to delinquent debts, and any information in the records, may be disclosed to Treasury pursuant to the Debt Collection Improvement Act of 1966, Pub. L. 89-104-134, for the purpose of locating the debtor and/or effecting administrative offset against monies payable by the Government to the debtor, or held by the Government for the debtor, to recover such delinquent debts.

(e) To notify client agencies as to the status of payments and to make inquiries and representations as necessary during the processing of debt collection payments, whether such payments are made voluntarily or whether they are collected through the tax refund offset procedure.

(f) To contractor employees operating the Nationwide Central Intake Facility to account for and report debtor payments that have been received. (See the "Debt Collection Management System" (Justice/JMD-006" which describes debtor records maintained by the Nationwide Central Intake Facility.)

(g) In a proceeding before a court or adjudicative body before which DOJ or contract private counsel are authorized to appear when any of the following is a party to litigation or has an interest in litigation and such records are determined by DOJ or contract private counsel to be arguably relevant to the litigation: (1) DOJ, or any component thereof, or contract private counsel, or (2) any employee of DOJ or contract private counsel in his or her official capacity, or (3) any employee of DOJ or contract private counsel in his or her individual capacity when DOJ has agreed to represent the employee, or (4) the United States, where DOJ or contract private counsel determines that the litigation is likely to affect DOJ or any of its components.

(h) To volunteer student workers and students working under a college work-study program where it is necessary to enable them to perform their duties.

(i) To employees or to contract personnel to access the records for Privacy Act training purposes.

(j) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(k) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record.

(l) To the National Archives and Records Administration (NARA) and to the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Periodic reports are stored in binders; automated data is stored on magnetic tape.

Retrievability:

Records are retrieved by debtor's name or TIN.

Safeguards:

Access to the facility where the records are maintained requires identification clearance by a security officer or guard. Paper records are maintained in a locked room during non-duty hours. Access to automated data requires the use of the proper passwords and user identification codes by personnel with security clearances. Finally, only those personnel who require access to perform their duties may access these records.

Retention and disposal:

Paper records are shredded after five years; automated information will be erased ten years after the related case files reported in the Debt Collection Enforcement System, Justice/USA-015, have been closed. (Pending approval of the NARA).

System manager(s) and address:

Deputy Assistant Attorney General, Debt Collection Management, Justice Management Division, Department of Justice, Washington, DC 20530.

Notification procedure:

Address requests to the system manager identified above.

Record access procedures:

Address requests for access to the system manager identified above. Clearly mark the envelope "Privacy Access Request." Include in the request the debtor's name, TIN, address and any other identifying information which may be assistance in locating the record, e.g., name of the case or Federal agency to whom the debtor is indebted. In addition, include notarized signature of the debtor as well as the name and address of the individual to receive the information if other than the debtor.

Contesting record procedures:

Address requests to contest to the system manager identified above. State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment to the information.

Record source categories:

USAs on behalf of Federal agencies; DOJ components; DOD, USPS, IRS, and the debt

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)**JUSTICE/JMD-016**

SYSTEM NAME:

Employee Assistance Program (EAP) Counseling and Referral Records, Justice/JMD-0

SYSTEM CLASSIFICATION:

Not classified.

SYSTEM LOCATION:

The Justice Management Division, EAP staff, maintains records. Interested parties wishing to correspond regarding records should direct their inquiries to the EAP System Manager, Workforce Support Group, Justice Management Division, U.S. Department of Justice, 900 Pennsylvania Ave., NW., Washington, DC 20530, or call (202) 514-1846.

Categories of individuals covered by the system:

Current and former employees of the Offices, Boards, Divisions and occasionally Bureaus of the Department (as listed at 28 CFR 0.1), including the Office of the Inspector General, Executive Office of the U.S. Trustees, the Executive Office for Immigration Review and the Office of Justice Programs, who have sought counseling or have been referred for counseling or treatment through the EAP. To the limited degree that counseling and referral may be provided to family members of these employees, these individuals are covered by the EAP System. The remainder of this notice will refer to all persons covered by the System as client(s)."

Categories of records in the system:

Records include any record, written or electronic, which may assist in diagnosing, evaluating, counseling and/or treating an EAP client, or resolving an EAP client's complaint or management's concerns (management consultation) regarding the EAP client's performance, attendance, or conduct problems. Included are the EAP counselor's intake/termination and outcome documents; case notes; pertinent psychosocial, medical and employment history.

medical tests or screenings, including drug and alcohol tests and information on positive tests generated by the staff of the Drug Free Workplace Program or treatment facilities which the EAP client may be receiving treatment; treatment and rehabilitation plans; behavior improvement plans; and records of referrals. Referrals include those to community treatment resources and social service agencies that provide legal, financial or other assistance not related to mental health or general medical services. Where clinical referrals have been made, records may include relevant information related to counseling, diagnosis, prognosis, treatment and evaluation, together with follow-up data that may be generated by the community programs providing the relevant services. Other records included in the system are the written correspondence forms used to permit the disclosure of information outside the EAP. Records may also include account information, such as contractor billings and government payments, when EAP services are provided by an EAP contractor.

Authority for maintenance of the system:

42 U.S.C. sec. 290dd-2; 42 CFR part 2; 5 U.S.C. 3301, 7361, 7362, 7901 and 7904; 44 U.S.C. 3101; Executive Order 12564; and Pub. L. 100-71, 101 Stat. 391, sec. 503 (July 11, 1987).

Purpose(s):

Records are maintained to document the work performed by the EAP on behalf of the EAP client and to allow for the tracking of the EAP client's progress and participation in the EAP community programs. These records may also be used to track compliance with Abeyaratne Last Change Agreements that include treatment options, in which the EAP is an integral part of establishing and/or monitoring treatment compliance as directed by the EAP client.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

In addition to those disclosures permitted by the Privacy Act itself, 5 U.S.C. 552a(b), relevant information may be disclosed from this system of records without EAP client consent as follows: 1A\1\

1. To appropriate State or local authorities to report, where required under State law, incidents of suspected child, elder or domestic abuse or neglect.
2. To any person or entity to the extent necessary to prevent an imminent crime which could result in the death or serious physical injury of any person.

threatens loss of life or serious bodily injury.

3. To JMD contractors that provide counseling and other services through referrals from EAP staff to the extent that it is appropriate, relevant, and necessary to enable the contractor to perform his or her counseling, treatment, rehabilitation, and evaluation responsibilities.

4. To any person who is responsible for the care of an EAP client when the EAP client's records pertain to a person who is mentally incompetent or under legal disability.

5. To any person or entity to the extent necessary to meet a bona fide medical emergency.

Disclosure to consumer reporting agencies:

Not Applicable.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Information in this system is maintained on paper and computer discs which are stored in locked GSA-approved security containers.

Retrievability:

Records are indexed and retrieved by identifying number or symbol, cross-indexed to EAP client names.

Safeguards:

Paper records and computer discs are kept in locked GSA-approved security containers. The computer discs are password protected. Only EAP staff will have access to the records. Records may be reviewed by any EAP staff member as may be needed to provide EAP services. No record may be released by the DOJ EAP staff without prior approval of the EAP System Manager.

Retention and disposal:

Records are retained for three years after the EAP client ceases contact with the counselor in accordance with General Records Schedule No. 1, Item No. 26) unless a longer retention period is necessary because of administrative or judicial proceedings. In such cases, the records are retained for six months after the conclusion of the proceedings. Paper records are destroyed by shredding, which must be performed by an EAP staff member. Computer records are erased, degaussed or physically destroyed by an EAP staff member.

System manager(s) and address:

DOJ Workforce Support Group, Assistant Director, Justice Management Division, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530, or call (202) 514-1846.

NOTIFICATION PROCEDURES:

Same as Record Access Procedures.

Record access procedures:

Make all requests for access in writing to the EAP System Manager identified above. Clearly mark the envelope and letter "Freedom of Information Act/Privacy Act Request." Provide the name and notarized signature of the individual who is the subject of the record, the date during which the individual was in counseling, any other information which may assist in identifying and locating the record, and a return address.

Contesting record procedures:

Direct all requests to contest or amend information to the EAP System Manager identified above. The request should follow the Record Access Procedures, listed above, and should state clearly and concisely the information being contested, the reason for contesting it, the proposed amendment thereof. Clearly mark the envelope and letter "Freedom of Information Act/Privacy Act Request."

Record source categories:

Records are generated by EAP personnel, referral counseling and treatment programs

individuals, the EAP client who is the subject of the record, the personnel office and the client's supervisor. In the case of drug abuse counseling, records may also be generated by the staff of the Drug-Free Workplace Program and the Medical Review Officer.

Exemptions claimed for this system:

None.

[\[TOP\]](#)

JUSTICE/JMD-017

System name:

Department of Justice (DOJ) Employee Transportation Management System, Justice/JMD-017

System location:

Records are located in the offices of the Employee Transportation Coordinator of the relevant DOJ components as listed in Appendix I of Part 16, 28 CFR. Records may also be maintained at individual DOJ facilities or regional offices.

Categories of individuals covered by the system:

Covered are any individuals who may apply for or participate in the ridesharing, parking transportation benefit programs of the DOJ. The term "transportation benefits" include the transit subsidy program and the transportation fringe benefits (tax exclusion) program. Individuals include: (1) DOJ employees and other federal and non-federal agency employees and applicants for, and/or recipients of ridesharing information; (2) DOJ employees and other federal and non-federal agency employees and applicants for, and/or recipients of parking privileges; (3) DOJ employees and other federal and non-federal agency employees who may participate as riders in the parking program with DOJ employees who have applied for or who have been granted parking privileges; (4) DOJ employees and other federal and non-federal agency employees and applicants for, and/or recipients of transportation benefits and authorized use of home-to-work transportation.

DOJ employee applicants and recipients may include former DOJ employees; non-federal employees may include private sector and other state and local government employees

Categories of records in the system:

Records in the system include any records necessary to carry out the responsibilities authorized by law related to parking, ridesharing, and transportation benefit programs.

Paper records may include DOJ car/vanpool parking space applications and written req for executive, unusual and handicapped parking assignments; ridesharing applications provide or request application information related to availability for car/vanpools, and/or provide or request similar information related to potential car/vanpool members; transpo benefit program applications and certifications; correspondence to applications; docum of usage; tax information related to participation in the transportation benefit programs; Air Act information and paperwork documenting compliance with state requirements; an administrative reports—including status reports and reports of disbursements to transpo benefit program participants.

Paper records may also include the notifications described under "Routine Uses of Rec Maintained in the System, *FOUO*."

Computer records may include data from the employee applications and/or from person records. Data from personnel records may include any data needed to process an application—such as that needed to verify employment, e.g., federal service computatio organization code, or that needed to identify parking assignments or fare subsidies that longer valid, e.g., separation date.

Authority for maintenance of the system:

5 U.S.C. 301; Executive Order 12191 of February 1, 1980, on the Federal Facility Rides Program; the Federal Employees Clean Air Incentives Act (5 U.S.C. 7905), effective Jan 1994; Treatment of Employer-Provided Transportation Benefits (26 U.S.C. 132 et seq.), effective December 31, 1992; the Clean Air Act (42 U.S.C. 7418) regarding employee-ov vehicles operated on federal facilities; and transportation benefit programs required by Executive Order 13150.

Purpose(s):

Information in the system will be used to assign, manage, and control the use of vehicle

parking spaces and the issuance of transportation benefits; to assist employees and the in forming car/vanpools; to ensure compliance with the clean Air Act; and to ensure the integrity of the parking and transportation benefit programs of the Department of Justice and other federal agencies by validating parking assignments and transportation benefit program requests.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant records may be disclosed:

- (1) As is necessary to respond to congressional inquiries on behalf of constituents;
- (2) To the National Archives and Records Administration in records management inspections conducted under the authority of Title 44 U.S.C. 2904 and 2906;
- (3) To DOJ employees to enable them to contact other individuals covered by this system of records for the purpose of forming or participating in car/vanpool.
- (4) To federal agencies and/or to the Metropolitan Council of Governments, and similar organizations, to enable such organizations—through coordinating efforts with other federal agencies—to provide information to any person for the purpose of contacting any individual covered by this system of records in order to form or participate in a car/vanpool. Disclosure may include a list of program participants or, where appropriate, it may relate to only one or multiple individuals.
- (5) To state transportation organizations, in summary form, in compliance with Clean Air Act requirements and Departmental guidelines.
- (6) To federal agencies and DOJ parking and transportation benefit program managers. Parking spaces may be assigned according to a variety of established priorities among federal agencies and, in some instances, according to specific criteria, e.g., carpools with the greatest number of participants (except in a tie). Therefore, these disclosures would enable other federal agencies and DOJ to review the validity of parking space assignments, identify and take appropriate action with respect to those who violate parking assignment policies (as set forth in published agency operating procedures and policies), and thus allocate spaces accordingly. In addition, because transportation benefits are offered to encourage the use of public

transportation for those not allocated parking privileges, such disclosures would also ensure that both parking privileges and transportation benefits are not provided to the same employee(s), unless otherwise authorized.

(7) To federal agencies, DOJ may also provide information as follows:

DOJ Employee Information:

(a) Upon request, either a list of DOJ employees, or an affirmative, negative or "non-DOJ employee" response as to whether or not a DOJ employee(s) (or name represented to be a DOJ employee)—is listed as a participant (or as an applicant) in DOJ's parking or transportation benefit programs; or is authorized to use a DOJ vehicle for home-to-work transportation (or has requested such authorization). Disclosure is made to enable that agency to determine or validate a DOJ employee's eligibility to participate in its parking program.

(b) Upon DOJ initiative, either a DOJ employee name(s) or a list on which DOJ employees are named as participants (or as applicants) in DOJ's parking or transportation benefit program or as employees authorized to use a DOJ vehicle for home-to-work transportation (or as employees who have requested such authorization). Disclosure is made to elicit an affirmative or negative response as to whether such DOJ employee(s) participate with another federal agency employee in that agency's parking program (or have requested such participation) thus enable DOJ to determine or validate DOJ employee eligibility for any form of DOJ parking privileges, or for DOJ transportation benefits.

Other Federal Agency Employee Information:

(c) Upon request, either a list of another federal agency's employees or an affirmative or negative response as to whether or not such employee(s) participate (or have requested participation) in DOJ's parking program. Disclosure is made to enable that agency to determine or validate eligibility for any form of parking privileges, or transportation benefits, for its employees.

(d) Upon DOJ initiative, either a federal agency employee name(s) or a list on which such agency's employee(s) are named as participating in DOJ's parking program (or has requested such participation). Disclosure is made to elicit from that agency an affirmative, negative

"non-employee" response as to whether such employee(s) participate (or have requested participation) in that agency's parking or transportation benefit programs, or are authorized to use a vehicle for home-to-work transportation (or have requested such authorization), and enable DOJ to determine or validate other federal agency employee eligibility to participate in DOJ's parking program.

(e) To the Internal Revenue Service any document which provides information related to tax matters.

Non-Federal Employee Information:

(f) Upon request, either the name(s) of non-federal employees, a list of names or a list which includes their name(s). Disclosure is made to enable the agency to determine whether a non-federal employee may also be listed as a rider in DOJ's parking program and, as a result, enable the agency to determine or validate parking permit eligibility for its employees.

(g) Upon DOJ initiative, either the name(s) of non-federal employees, a list of names, or a list which includes their name(s). Disclosure is made to enable the DOJ to determine whether non-federal employees may also be listed as a rider in that agency's parking program and, as a result, enable the DOJ to determine or validate parking permit eligibility for DOJ employees.

(8) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

(9) Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are stored in hard copy form and/or electronically.

Retrievability:

Records may be retrieved by individual name, social security number, residential zip code, vehicle tag number, vehicle type, or other information from the application or personnel records. Records may be retrieved by name or other identifier directly and/or by asking the system to segregate a list, by name, of those who work for a particular DOJ component. Former DOJ employee names are retrieved by asking the system to segregate a list, by name, of those parking participants who have separated from employment with DOJ. Other federal agency employee names are retrieved by asking the system to segregate a list, by name, of those parking participants who are identified as employees of a particular federal agency. Non-federal agency employee names may be similarly segregated.

Safeguards:

These files are stored in locked file cabinets in secured facilities, and access is restricted to personnel having an official need. Automated records are protected through computer password security.

Retention and disposal:

Automated data is deleted from a data base within 180 days after any recordkeeping documents have been produced when the individual covered by the system no longer participates in the Employee Transportation Management program, e.g., when the employee is no longer on the ridesharing listing; is no longer a member of a car/vanpool; or, no longer receives a transportation benefit. Parking permit credentials shall be destroyed three months after the parking permits have either expired or been returned (General Records Schedule 1). Documents relating to the administration of the transit subsidy program and the transportation fringe benefit program shall be destroyed after the documents are three years old (General Records Schedule 9). Documents in either paper or electronic form relating to the disbursement of transportation pre-tax benefits to employees shall be destroyed after six years as approved by the National Archives and Records Administration.

System manager(s) and address:

Director, Facilities and Administrative Services Staff, Justice Management Division, NPB 1070, Department of Justice, Washington, DC 20530.

Notification procedure:

Individuals wanting to know whether information about them is maintained in this system records may review their own ridesharing, parking, transportation benefit, or other personal data upon presentation of a picture identification card at the appropriate address indicated under "Records Access Procedures."

Record access procedures:

Except as otherwise noted, employees of the Offices, Boards, and Divisions (listed in appendix I of part 16, 28 CFR) may appear in person or address their requests for access to: Employee Transportation Coordinator, Facilities and Administrative Services Staff, Justice Management Division, NPB Suite 1070, Department of Justice, Washington, DC 20530.

Except as otherwise noted, employees of the bureaus (listed in appendix I of Part 16, 28 CFR) may appear in person or address their requests for access to the following bureau official attention Employee Transportation Coordinator: Director, Bureau of Alcohol, Tobacco, Firearms, and Explosives, 650 Massachusetts Avenue, NW., Washington, DC, 20226.

Director, Bureau of Prisons, HOLC Building, 320 First Street, NW., Washington, DC 20535

Administrator, Drug Enforcement Administration, 700 Army Navy Drive, Arlington, VA 22202

Director, Federal Bureau of Investigation, J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW., Washington, DC 20535-0001

Director, U.S. Marshals Service, 600 Army Navy Drive, Arlington, VA 22202.

In those cases where parking or transportation benefit records are maintained at an individual DOJ facility or regional office, the parking or transportation coordinator at that facility or office should be contacted first.

Individuals who park in a DOJ building (or DOJ-leased space) other than the one in which

work, may review their parking record by presenting the required identification to the En Transportation Coordinator at the appropriate building address.

Contesting record procedures:

Individuals may request changes to their own record by submitting the proposed change in writing at the appropriate address indicated under "Records Access Procedures." Individuals who submit proposed changes to information provided by third parties should be prepared to provide information supporting their contention that such third-party information is erroneous.

Record source categories:

DOJ and other federal agency applicants; DOJ personnel records; state transportation organizations; participating Department components and other federal agencies.

System exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/JMD-019

System name: Freedom of Information Act-Privacy Act (FOIA-PA) Records System.

System location:

U.S. Department of Justice, Justice Management Division, 10th and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

Persons who have made a request to access any Justice Management Division (JMD) records relating to JMD functional responsibilities and activities; individuals who have made a request to access or correct records pertaining to themselves which they believed to be in JMD systems of records; and persons who, on behalf of another individual, have made a request to access or correct that individual's records which they believed to be in JMD systems of records.

requests were made pursuant to the Freedom of Information Act, the Privacy Act, or both.

Categories of records in the system:

Manual records contain Freedom of Information Act and Privacy Act requests for JMD responses thereto, and where applicable, a copy of the records requested and any other correspondence or internal memoranda related to the processing of these requests. Automated records (stored on disks) contain summary data such as the date of request, name of requester, addressee, subject of request, date request was received, JMD staff to which request were assigned, date request was assigned, date response was due, control number and date of response.

Authority for maintenance of the system:

This system is established and maintained pursuant to 44 U.S.C. 3101 and is maintained to implement the provision of 5 U.S.C. 552 and 552a and the provision of 28 CFR 16.1 et seq. and 28 CFR 16.40 et seq.

Purpose(s):

To assist the Justice Management Division in carrying out its responsibilities under the Freedom of Information Act and the Privacy Act.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in the system may be disseminated as a routine use of such records as follows: (1) A record may be disseminated to a Federal agency which furnished the record for the purpose of permitting a decision as to access or correction to be made by that agency; (2) a record may be disseminated to any appropriate federal, state, local, or foreign agency for the purpose of consulting with that agency as to the propriety of access or correction; (3) a record may be disseminated to any appropriate federal, state, local, or foreign agency for the purpose of verifying the accuracy of information submitted by an individual who has requested amendment or correction of records, contained in a system of records maintained by the Justice Management Division.

Release of information to the news media:

Information permitted to be released to the news media and the public pursuant to 28 C.F.R. 17.2 may be made available from systems or records maintained by the Department of Justice, unless it is determined that release of the specific information in the context of a particular request would constitute an unwarranted invasion of personal privacy.

Release of information to members of congress:

Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Members' behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Service Administration (GSA):

A record from a system of records may be disclosed as a routine use to NARA and GSA for records management inspections conducted under the authority of 44 U.S.C. 2904 and 44 U.S.C. 2905.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Manual requests records are stored in locked safes. Automated requests records are stored on hard disks.

Retrievability:

Requests records are filed and retrieved under the names of those persons and individuals identified under the caption "Categories of individuals covered by the system. These records are retrieved by Department personnel to perform their duties, e.g., when subsequent requests are made by the public for copies of their previous requests and responses thereto, or when the requester submits a supplemental request to information clarifying a previous request.

Safeguards:

Access to requests records is limited to Department of Justice personnel who have need for these records to perform their duties. Request files (manual records) are stored in locked safe and electronic records are stored in an office which is occupied during the day and locked at night.

Retention and disposal:

Records are disposed of in accordance with items 16 through 18 and 25 through 28 of the General Records Schedule 14.

System manager(s) and address:

Assistant Attorney General for Administration, U.S. Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Same as the System Manager.

Record access procedures:

A request to access a record in this system shall be made in writing to the system manager named above with the envelope and letter clearly marked "Freedom of Information Act request" or "Privacy Act request." The requester shall include the full name of the person who made the request, date of that request, name of official to whom the request was addressed, and subject of the request. Where applicable (Title 28 of the Code of Federal Regulations section 1606(2) and (3)), the requester shall also include the current address, date and place of birth, and notarized signature of the individual requesting a copy of his/her previous request and response thereto. Where applicable (Title 5 of the United States Code, section 552a(b))

requester shall also include a written statement authorizing the Department to release the records to a third party. In addition, the requester shall provide his return address.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the system manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

The sources of information contained in this system are the individuals and persons making requests, the systems of records searched in the process of responding to requests, and agencies referring requests for access to or correction of records originating in the Justice Management Division.

Systems exempted from certain provisions of the act:

The Attorney General has exempted certain categories of records in this system from subsections (c)(3) and (d) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). That is, the exemptions apply only to the extent that other correspondence or internal memoranda with the request file contain investigatory material for law enforcement purposes. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/JMD-022

System Name

Department of Justice Consolidated Asset Tracking System (CATS).

Security Classification:

Sensitive-But-Unclassified (SBU).

System Location

U.S. Department of Justice, Asset Forfeiture Management Staff, Washington, D.C. 20535

Categories of Individuals Covered by the System

The system covers persons involved with the ownership of or claims upon property seized for forfeiture under specified Federal statutes and law enforcement policies, including owners, individuals possessing or controlling the property, other parties provided notification of the seizure, lienholders, parties filing claims in contest of the seizure, petitioners, U.S. Attorney, investigative agents and contractors of the Federal Government.

Categories of Records in the System

Name, address, phone number, Social Security number, and other identifying information of persons referenced in records pertaining to the administration, seizure, custody, notification, claim, petition, forfeiture, disposal, equitable sharing, official use, income and expenses, service of process, and abandonment of property seized for forfeiture.

Authority for Maintenance of the System

28 U.S.C. 524(c); 44 U.S.C. 3101.

Purpose of the System

CATS supports the Federal Government participants in Department of Justice's (DOJ) Asset Forfeiture Program by meeting their operational and management reporting needs for all phases of the asset forfeiture life-cycle including the following major business processes: seizure of forfeitable assets; transfer and custody of seized assets; automation of legal notification and publication requirements; receipt and processing of claims contesting the government's grounds for forfeiture; petition receipt and processing; litigation and administrative proceedings culminating in asset forfeiture, disposal, and equitable sharing.

CATS is an inventory database which stores and processes asset forfeiture data maintained by the Department of Justice (DOJ). Some of the data are owned by other agencies of the Federal Government, and DOJ serves as custodian for the data.

Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses:

Relevant CATS data may be disclosed as follows:

(1) Law enforcement information may be disclosed to any criminal, civil, or regulatory law enforcement authority (whether Federal, state, local, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

(2) Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, state, local, foreign, or tribal, law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.

Relevant information may be disclosed:

(3) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system's records.

(4) To a former employee of the Department for purposes of: responding to an official inquiry by a Federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(5) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

(6) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Disclosure to Consumer Reporting Agencies:

Not Applicable.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing Records in the System:***Storage:***

Records are stored in electronic form and on paper.

Retrievability:

Information is retrieved by unique asset identifiers, to include names of individuals (if applicable), Social Security Numbers and Tax Identification Numbers.

Safeguards:

Information in this system is safeguarded in accordance with applicable rules and policies including the Department's automated systems security and access policies. In general records and technical equipment are maintained in buildings with restricted access. The required use of password protection identification features and other system protection methods also restrict access. Access is limited to those who have an official need for access to perform their official duties.

Retention and Disposal:

There are over 820,000 records stored in the system. A request for Records Disposition Authority is pending with the National Archives and Records Administration.

System Manager and Address:

Assistant Director of Systems (CATS), Asset Forfeiture Management Staff, Justice Management Division, Department of Justice, 20 Massachusetts Ave., NW, Washington 20530

Notification Procedures:

Address inquiries to System Manager named above.

Record Access Procedures:

Requests for access must be in writing and should be addressed to the System Manager named above. The envelope and letter should be clearly marked "Privacy Act Access Request."

The request should include a general description of the records sought and must include requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury.

Contesting Record Procedures:

Individuals desiring to contest or amend the information maintained in the system should submit their request according to the Records Access procedures and to the System Manager named above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record Source Categories:

Sources of information contained in these systems include DOJ and other Federal Agencies participating in the DOJ Asset Forfeiture Program.

Exemptions Claimed for the System:

None.

[\[TOP\]](#)

Justice/JMD-023

System name:

Federal Bureau of Investigation Whistleblower Case Files.

Security classification:

The system itself is not classified. However, items or records within the system may have national security/foreign policy classifications.

System location:

Records in this system are located at the Department of Justice, Justice Management Office of Attorney Recruitment and Management (OARM), 20 Massachusetts Avenue, N Suite 5100, Washington, DC 20530.

Categories of individuals covered by the system:

The records in the system relate to OARM's adjudication of FBI whistleblower cases, and customarily include: requests or recommendations for corrective action brought pursuant to 28 CFR Part 27; the parties' written comments, pleadings, and/or motions, correspondence between OARM and the parties and OARM and the Conducting Offices; lists of witness evidence and exhibits (to include written documentation, audiotapes, and/or videotapes); deposition and hearing transcripts; OARM's Opinions and Orders; and any directive and decision by the Deputy Attorney General.

Categories of records in the system:

The records in the system relate to OARM's adjudication process and customarily include: an employee's request for corrective action (or OIG's/OPR's recommendation for corrective action); the parties' submissions, correspondence between OARM and the parties, and OARM's Opinions. These records may also include, but are not limited to, status conference transcripts and evidentiary submissions and exhibits (e.g., affidavits, depositions, video/audio tapes, electronic communications, newspaper articles, etc.). Records in the system may also include OIG/OPR Reports of Investigation, including those that serve to terminate an investigation of an alleged unlawful reprisal (subject to 28 CFR 27.3(h) and (i)).

Authority for maintenance of the system:

5 U.S.C. 301; 44 U.S.C. 3101; 28 CFR Part 27.

Purpose(s):

The system maintains all documents and evidence filed with the Director of OARM pertaining to the adjudication of FBI whistleblower cases.

requests for corrective action by employees of, or applicants for employment with, the FBI; recommendations for corrective action by OIG/OPR) brought under the FBI's whistleblower regulations, 28 CFR Part 27. The records in the system are used by the Director of OAF to determine whether an employee or applicant made a protected disclosure that was a contributing factor in the FBI's decision to take (or fail to take, or threaten to take or fail to take) a covered personnel action against the employee or applicant and, if so, what, if any, corrective action can and should be appropriately ordered.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records or information from this system of records may be disclosed under the following circumstances when it has been determined by the Department of Justice that such a disclosure exists:

1. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.
2. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests information on behalf of, and at the request of, the individual who is the subject of the record.
3. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904, 2906.
4. Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, foreign, or tribal law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.
5. In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

6. To an actual or potential party to litigation or administrative proceeding, or to the party's authorized representative, for the purpose of negotiation or discussion of such matters or settlement, plea bargaining, or in informal discovery proceedings.
7. To appropriate officials and employees of a Federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.
8. To Federal, State, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.
9. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.
10. To a former employee of the Department for purposes of: responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes for which the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Disclosure to consumer reporting agencies:

Not applicable.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are maintained in hard copy and in electronic form accessible with office authorization.

software on Department personal computers within OARM's office suite.

Retrievability:

Information is retrieved by the name of the individual who has filed a request for corrective action with OARM (or for whom OIG or OPR has made a recommendation for corrective action to OARM) pursuant to a claim of unlawful reprisal brought under the FBI whistleblower regulations, 28 CFR Part 27.

Safeguards:

Information in this system is safeguarded in accordance with applicable rules and policies including the Department's automated systems security and access policies. Records in this system are maintained in restricted access space in Department of Justice controlled facilities and offices. All physical access to the building where this system of records is maintained is controlled and monitored by security personnel. Computerized data is password protected and information is accessed only by authorized Department personnel or by non-Department personnel properly authorized to assist in the conduct of an agency function related to this system of records.

Retention and disposal:

PERMANENT. Transfer to the Washington National Records Center two years after closing. Transfer to the National Archives 10 years after closing.

System manager(s) and address:

Director, Office of Attorney Recruitment and Management, Justice Management Division
Department of Justice, 20 Massachusetts Avenue, NW., Suite 5100, Washington, DC 20530

Notification procedure:

Address inquiries to the System Manager named above.

Record access procedures:

Requests for access must be in writing and should be addressed to the System Manager.

named above. The envelope and letter should be clearly marked "Privacy Act Request." Requests for access to records must comply with the Department's Privacy Act regulations. Requests must include a general description of the records sought, and the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. Some information may be exempt from provisions as described in the section entitled "Exemptions Claimed for the System." An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request according to the Records Access procedures and to the System Manager, stating clearly and concisely what information is being contested, the reasons for contesting, and the proposed amendment to the information sought. Some information may be exempt from contesting record procedures as described in the section entitled "Exemptions Claimed for the System." An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

Record source categories:

Information in this system of records is obtained from the subject of the record and/or the subject's representative, the FBI, officials of the Department, and official Department documents.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (3), and (4); (e)(1), (2), (3), (5) and (8); and (g). The exemptions will be applied only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j)(1) and (k). A determination as to exemption shall be made at the time a request for access or amendment is received. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e), and have been published in the *Federal Register*.

[\[TOP\]](#)

JMD-024

SYSTEM NAME:

Attorney Student Loan Repayment Program Applicant Files, Justice/JMD-024.

SECURITY CLASSIFICATION:

The information in this system is not classified.

SYSTEM LOCATION:

Records in this system are located at the Department of Justice, Justice Management Office of Attorney Recruitment and Management, 20 Massachusetts Avenue, NW., Suite 1200, Washington, DC 20530.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system contains records and related correspondence on persons serving in or hire to serve in a Department attorney position who submit applications for participation in the Attorney Student Loan Repayment Program (ASLRP), as well as attorneys who have been previously approved for and who are presently receiving or previously have received such benefits.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records may include: employees' (or potential employees') names, home and work addresses, social security numbers, student loan account numbers, loan balances, repayment schedules, repayment histories, and repayment status. They may also include loan holders' names and addresses, and telephone numbers, Employee Service Agreements, justifications, and correspondence relating to employees' (or potential employees') applications.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The system is based on the provisions of 5 U.S.C. 5379, as amended.

PURPOSE(S):

The ASLRP is an agency recruitment and retention incentive program. Based on the provisions of 5 U.S.C. 5379, as amended, the ASLRP is an incentive program designed to recruit and retain highly qualified attorneys for hard-to-fill positions. Any Department of Justice employee serving in or hired to serve in an attorney position may request consideration for the ASLRP.

Records in this system are necessary in order for the Department to determine the eligibility of each applicant requesting consideration for a student loan repayment. These records are maintained to determine eligibility and benefits and to process requests to receive student loan repayments. The records are also used by the Department to prepare its reports for the Office of Personnel Management (OPM), as required by 5 CFR 537.110.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Records or information from this system of records may be disclosed under the following circumstances when it has been determined by the Department of Justice that such a disclosure exists:

1. To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.
2. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests information on behalf of, and at the request of, the individual who is the subject of the record.
3. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.
4. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.
5. In an appropriate proceeding before a court, or administrative or adjudicative body, with

Department of Justice determines that the records are arguably relevant to the proceeding in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

6. To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings.

7. To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance, the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

8. To federal, state, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

9. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

10. To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

11. To OPM, any records or information in this system of records that OPM requests or requires pursuant to OPM's oversight and regulatory functions.

12. To other Federal agencies, hearing or court officials, and present employers of an employee in order for the Department to obtain repayment, if an employee fails to complete a period of employment under a service agreement and fails to reimburse the Department.

amount of any student loan repayment benefits the employee received from the Department.

13. To the Department's payroll processing provider in order to calculate tax withholding and disburse payments of student loan repayment benefits to loan holders on behalf of employees approved to receive this benefit.

14. To student lending institutions or loan holders in order to obtain information (such as a borrower's account number, original and current loan balance, repayment schedule, repayment history, and current repayment status) to allow the Department to determine employee's or potential employee's initial and continuing eligibility for this program, to facilitate accurate payments to student loan holders on behalf of eligible employees, and to ensure the Department discontinues making student loan repayments to individuals who do not remain eligible for them during the period of the service agreement.

15. To any criminal, civil, or regulatory law enforcement authority (whether federal, state, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

16. To appropriate agencies, entities, and persons when (1) it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Not applicable.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are maintained in hard copy and in electronic form accessible with office automation software on Department computers within OARM's office suite.

RETRIEVABILITY:

Information is typically retrieved by name of the individual, or other personal identifiers (social security number).

SAFEGUARDS:

Information in this system is safeguarded in accordance with applicable rules and policies including the Department's automated systems security and access policies. Records in the system are maintained in restricted access space in Department controlled facilities and offices. Computerized data is password protected. The information is accessed only by authorized Department personnel or by non-Department personnel properly authorized to assist in the conduct of an agency function related to these records. All physical access to the building where these records are maintained is controlled and monitored by security personnel.

RETENTION AND DISPOSAL:

The retention and disposal schedule for these records is pending approval of the National Archives and Records Administration.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Office of Attorney Recruitment and Management, Justice Management Division
Massachusetts Avenue, NW., Suite 5100, Washington, DC 20530.

NOTIFICATION PROCEDURE:

Address inquiries to the System Manager named above.

RECORD ACCESS PROCEDURE:

Requests for access to a record from this system must be in writing and should be addressed to the System Manager named above. The envelope and the letter should be clearly marked "Privacy Act Request." Requests for access to records must comply with the Department's

Privacy Act regulations, to include a general description of the records sought, and the requester's full name, current address, and date and place of birth. The request must be signed and dated, and either notarized or submitted under penalty of perjury. The requester may submit any other identifying data he/she wishes to furnish to assist in making a precise search of the system.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in this system should direct their requests according to the Records Access procedures and to the System Manager, stating clearly and concisely what information is being contested, the reasons for contesting, and the proposed amendment to the information sought.

RECORD SOURCE CATEGORIES:

Information in this system of records is obtained from the individual to whom the information applies, lending institutions holding student loans for the individual to whom the information applies, officials of the Department, and official Department documents.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[\[TOP\]](#)

Environment and Natural Resources Division

JUSTICE/ENRD—001

System name:

Appraisers, Approved Attorneys, Abstractors and Title Companies Files Database System

Security classification:

Unclassified.

System location:

U.S. Department of Justice, Environment and Natural Resources Division, Land Acquisition Section, 601 Pennsylvania Avenue, NW, Washington, DC 20004.

Categories of individuals covered by the system:

(1) Appraisers who have prepared real property appraisals, whose work has been reviewed by the Appraisal Unit, Environment and Natural Resources Division, in conjunction with anticipated or pending litigation. (2) Attorneys, title abstractors, and title insurance companies that have applied and been deemed qualified to prepare title evidence for land acquisition in the United States.

Categories of records in the system:

This system includes automated records relating to (1) the qualifications of appraisers who have provided real estate appraisals to the Appraisal Unit, Environment and Natural Resources Division, in conjunction with anticipated or pending litigation; and (2) records relating to evidence providers, including applications, supporting information, and information relating to qualifications received by the Environment and Natural Resources Division.

Authority for maintenance of the system:

Authority to establish and maintain this system is contained in 28 U.S.C. 509 and 510, 28 U.S.C. 2512, part O, subpart M, and 40 U.S.C. 257 et seq., which authorize the Attorney General to conduct litigation, particularly proceedings for condemnation of property, and 5 U.S.C. 301 and 5 U.S.C. 3101, which authorize the Attorney General to create and maintain federal records management agency activities.

Purpose(s):

(1) Appraisal information is maintained so that an appraiser's credentials, experience, and performance can be referenced and evaluated when the Division seeks an appraiser for anticipated or pending litigation. (2) Title evidence information is maintained so that a provider's performance can be referenced when the Division seeks a qualified provider for work to be reviewed.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

(1) Records may be disclosed to the National Archives and Records Administration in re management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(2) Records relating to attorneys, abstractors, or title companies may be disclosed to oth Federal agencies to help them hire such professionals.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or profess licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assista from the former employee regarding a matter within that person's former area of respon

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Information is kept on a computer database.

Retrievability:

Information is retrieved by name of the subject, Department of Justice case number, ap review number, or land unit number.

Safeguards:

Only employees of the Land Acquisition Section with access to the Division computer sy have access to the system of records.

Retention and disposal:

Records are retained during their useful life subject to National Archives and Records Administration record retention schedules.

System manager(s) and address:

Chief, Land Acquisition Section, Environment and Natural Resources Division, U.S. Dep of Justice, 601 Pennsylvania Avenue, NW., Washington, DC 20004.

Notification procedure:

Address inquiries to the FOIA/Privacy Act Coordinator; Environment and Natural Resources Division; Law and Policy Section; PO Box 4390; Ben Franklin Station; Washington, DC 20044-4390.

Record access procedures:

Submit in writing all requests for access, and clearly mark the envelope and letter, "Privacy Access Request." Include in the request your full name, date, and place of birth, case number or other information which may assist in locating the records you seek. Also include your notarized signature and a return address. Direct all access requests to the FOIA/Privacy Act Coordinator; Environment and Natural Resources Division; Law and Policy Section; PO Box 4390, Ben Franklin Station; Washington, DC 20044-4390.

Contesting record procedures:

If you wish to contest or amend information maintained in the system, Direct your request to the FOIA/PA Coordinator Stating Clearly and concisely what information is being contested, reasons for contesting it, and the proposed amendment to the information you seek.

Record source categories:

The record subject is the principal record source. The sources may be supplemented by individuals having knowledge of the subject's professional qualifications.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

JUSTICE/ENRD-003

System name:

Environment and Natural Resources Division Case and Related Files System.

Security classification:

Unclassified.

System location:

Environment and Natural Resources Division, U.S. Department of Justice, 950 Pennsylvania Ave., NW, Washington, DC 20530; DC offices (601 D Street, NW, Washington, DC 20004; Pennsylvania Ave., NW, Washington, DC 20004; 1425 New York Ave., NW, Washington 20005; 801 Pennsylvania Ave., NW, Washington, DC 20004); field offices (in Anchorage, Alaska; Sacramento, CA; San Francisco, CA; Denver, CO; Newton Corner, MA; and Seattle, WA); Federal Records Center, Suitland, MD 20409.

Categories of individuals covered by the system:

(a) Individuals being investigated in anticipation of civil or criminal suits; (b) Individuals involved in civil or criminal suits; (c) Defense or plaintiff's counsel(s); (d) Information sources; (e) Individuals relevant to the development of civil or criminal suits, including expert and other witnesses; (f) Individual plaintiffs or defendants; and (g) Attorneys, paralegals, and other employees of the Environment and Natural Resources Division directly involved in these matters.

Categories of records in the system:

(1) Records in this system are established and maintained for litigation and related activities of the Environment and Natural Resources Division, including, but not limited to, the protection and development of natural resources and public lands, wildlife protection, Indian rights and claims, cleanup of hazardous waste sites, acquisition of private property for federal purposes, prosecution of environmental crimes, enforcement of environmental laws, and defense of

environmental challenges to government programs and activities. The case files contain records (such as briefs, motions, and orders), inter-agency and intra-agency correspondence, legal research, and other related documents. These records may include civil investigation and/or criminal law enforcement information and information classified pursuant to Executive Order to protect national security interests. (2) Summary information of these cases or records (such as names of principal parties or subjects, court docket numbers, status, and attorney assignments) is maintained in an automated case management system (CMS). (3) A timekeeping function for attorneys, paralegals, and other employees of the Environment and Natural Resources Division supplements the automated case management system.

Authority for maintenance of the system:

Authority to establish and maintain this system is contained in 5 U.S.C. 301 and 44 U.S.C. 3101, which authorize the Attorney General to create and maintain federal records of agency activities.

Purpose(s):

Case records are maintained to litigate or otherwise resolve civil or criminal cases or matters handled by the Environment and Natural Resources Division. The automated case tracking and timekeeping system are maintained to manage and evaluate the Division's litigation and activities.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

(a) In any case in which there is an indication of a violation or potential violation of law (civil, criminal, or regulatory in nature), the record may be disseminated to the appropriate federal, state, local, tribal, or foreign agency charged with the responsibility of investigating, defining or pursuing such violation, civil or criminal claim or remedy, or charged with enforcing, defending or implementing such law;

(b) In the course of investigating a potential or actual violation of any law, or during the trial or hearing of (or in preparation for) a trial or hearing for such a violation, a record may be disseminated to an individual, agency or organization, if there is reason to believe that such individual, agency or organization possesses relevant information relating to the investigation (or trial or hearing) and the dissemination is reasonably necessary to elicit information or to obtain the cooperation of such individual, agency or organization.

of a witness or an agency;

(c) A record relating to a case or matter may be disseminated in a federal, state, local, or administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing;

(d) A record relating to a case or matter may be disseminated to an actual or potential party, his or her attorney, or a third party neutral, for the purpose of negotiation or discussion of matters as settlement of the case or discussion on such matters as settlement of the case or matter, and for formal or informal discovery proceedings;

(e) A record relating to a case or matter that has been referred by an agency for investigation of a civil or criminal action, enforcement or defense, or that involves a case or matter within the jurisdiction of an agency, may be disseminated to such agency to notify the agency of the status of the case or matter, or of any decision or determination that has been made, or make such other inquiries and reports as are necessary during the processing of the case or matter;

(f) A record relating to a case or matter may be disseminated to a foreign country, through the United States Department of State or directly to the representative of such country, pursuant to an international treaty or convention entered into and ratified by the United States or to an executive agreement;

(g) A record may be disseminated to a foreign country, through the Department of Justice, the Federal Bureau of Investigation, United States Department of State, or directly to the representative of such country, to the extent necessary to assist such country in general crime prevention, the pursuit of criminal judicial actions or general civil regulatory or administrative actions, or to provide investigative leads to such country, or assist in the location and/or returning of witnesses or other evidence;

(h) A record, or facts derived from it, may be disclosed in a grand jury proceeding or in a proceeding before a court or adjudicative body before which the Environment and Natural Resources Division is authorized to appear when the United States, or any of its agencies or subdivisions, is a party to litigation, and the Environment and Natural Resources Division has determined that such records are arguably relevant to the litigation;

(i) Information permitted to be released to the news media and the public pursuant to 28

50.2 (Department of Justice regulations setting forth guidelines for disclosure of information to the media) may be made available from this system of records unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(j) A record may be disseminated to a federal, state, or local agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter;

(k) Pursuant to Subsection b(12) of the Privacy Act, records relating to an individual who owes an overdue debt to the United States may be disseminated to a federal agency which enforces the debt; a consumer reporting agency; a federal, state, local or foreign agency; or the Internal Revenue Service (IRS);

(l) Information contained in this system of records may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests information on the behalf of and at the request of the individual who is the subject of the records, even if the information would not otherwise be available under the Freedom of Information Act, 5 U.S.C. 552.

(m) Records may be disclosed to the National Archives and Records Administration in connection with management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(n) Information may be released to complainants or victims to the extent necessary to provide such persons with information and explanations concerning the progress or results of the investigation or case arising from their complaint or involvement as a victim.

(o) Timekeeping records may be disclosed to opposing parties and to courts in litigation regarding litigation costs.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating

communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Disclosure to consumer reporting agencies:

See Routine Use (k) listed above.

Policies and practices for storing, retrieving, accessing, retaining and disposing of information of the system:

Storage:

All information, except that specified in this paragraph, is recorded on computer files or paper/cardboard material that is stored in file folders, file cabinets, shelves, or safes. Some material is recorded and stored on other data processing storage forms.

Retrievability:

Information is retrieved primarily by name of the case or person, case number, complaint number or court docket number. Information within this system of records may be accessed by Environment and Natural Resources Division employees by means of the Case Management System (CMS) or successor systems.

Safeguards:

Information in the system is both confidential and nonconfidential and located in file cabinets at the Environment and Natural Resources Division offices in Washington, D.C., and field office locations. Information also is located in litigation support contract document centers and storage locations. Confidential materials are in locked file drawers and safes, and nonconfidential materials are in unlocked file drawers. Offices are secured by either Federal Protective Service or private building guards. Information that is retrievable by Environment and Natural Resources Division personnel trained to access the Case Management System or the time-keeping system or successor systems within various Environment and Natural Resources Division offices is password protected and requires access to the Department's secure Justice Consolidated Office Automation Network (JCON).

Retention and disposal:

Records are retained or disposed of after a case is closed in accordance with a retention/disposal schedule approved by the National Archives and Records Administration. The period that records are maintained ranges from 10 years after a matter is closed to permanently.

System manager(s) and address:

The System Manager is the Assistant Director, Office of Information Management, in coordination with the Office of Planning and Management's Records Management Unit.

Notification procedure:

Address inquiries to the FOIA/Privacy Act Coordinator; Environment and Natural Resources Division; Law and Policy Section; PO Box 4390; Ben Franklin Station; Washington, DC 20044-4390.

Record Access Procedures:

Portions of this system are exempt from disclosure and contest by 5 U.S.C. 552a(j)(2), (k) and/or (k)(2). An individual who is the subject of a record in this system may access the records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received. Submit in writing all requests for access, and clearly mark the envelope and letter, "Privacy Act Access Request." Include request your full name, date and place of birth, case caption, or other information which assist in locating the records you seek. Also include your notarized signature and a return address. Direct all access requests to the FOIA/Privacy Act Coordinator; Environment and Natural Resources Division; Law and Policy Section; PO Box 4390, Ben Franklin Station Washington DC 20044-4390.

Contesting record procedures:

Portions of this system are exempt from this requirement under 5 U.S.C. 552a(j)(2), (k) and/or (k)(2). An individual may contest those records that are not subject to exemption determination whether a record is exempt from contest shall be made at the time a request for contest is received. If you wish to contest or amend information maintained in the system

direct your request to FOIA/PA Coordinator stating clearly and concisely what information being contested, the reasons for contesting it, and the proposed amendment to the information you seek.

Record source categories:

Sources of information contained in this system include, but are not limited to investigation reports of client agencies of the Department of Justice; discovery materials; other than non-Department of Justice forensic reports; statements of witnesses and parties; verbatim transcripts of depositions and court proceedings; data, public reports, memoranda and from the court and agencies thereof; and the work product of Environment and Natural Resources Division Attorneys, Department of Justice attorneys, investigators, staff, and assistants working on particular cases or matters.

Exemptions claimed for the system:

The Privacy Act authorizes an agency to promulgate rules to exempt any system of records (or part of a system of records) from certain Privacy Act requirements, if the system of records is maintained by an agency which performs as its principal function any activity pertaining to the enforcement of criminal laws (5 U.S.C. 552a(j)(2)); it is investigatory material compiled for law enforcement purposes (5 U.S.C. 552a(k)(2)); or it is required by Executive Order to be kept secret in the interest of national defense or foreign policy (5 U.S.C. 552a(k)(1)).

Under these authorities, the Attorney General has promulgated rules to exempt those records in this system that pertain to the enforcement of criminal laws, that are investigatory material compiled for law enforcement purposes, or that are classified secret by an Executive Order from the following Privacy Act requirements: (1) The requirement under (c)(3) to make a response to the individual named in the record an accounting of the circumstances under which records about the individual were disclosed; (2) the requirement under (e)(1) to maintain only such information about an individual that is relevant and necessary to accomplish a purpose of the agency; and (3) the requirement under (f) to establish agency procedures to respond to an individual's request for information about himself. The Attorney General also has promulgated a rule to exempt records in this system compiled for criminal enforcement purposes from the following additional requirements: (1) The requirement under (c)(4) to inform any party or agency that receives an individual's records about any subsequent corrections made to the record; (2) the requirement under (e)(2) to collect information to the greatest extent practicable directly from the individual when the information may result in adverse determinations about an individual.

rights, benefits and privileges under Federal programs; (3) the requirement under (e)(3) to inform each individual from whom information is collected of the authority for the information, the principal purposes for the information, the routine uses, and the effects, if any, of not providing the information; (4) the requirement under (e)(5) to maintain all records with sufficient accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual, (5) the requirement under (e)(8) to make reasonable efforts to provide notice on an individual when any record on the individual is made available to any person under compulsory legal process when that process becomes a matter of public record; and (g) providing that individuals may bring a civil action against the agency for violations of the Privacy Act.

[\[TOP\]](#)

National Drug Intelligence Center

JUSTICE/NDIC-001

System name:

National Drug Intelligence Center Data Base (JUSTICE/NDIC-001).

System location:

The primary location of the system will be the National Drug Intelligence Center, 319 Washington Street, 5th Floor, Johnstown, PA 15907. In addition, information in the NDIC Data Base will be retrieved at the NDIC Washington area office, located at Suite 1001, 8201 Greensboro Drive, McLean, VA 22102.

Categories of individuals covered by the system:

1. Individuals suspected of, charged with, or convicted of, illicit narcotic trafficking or activities related thereto.
2. Non-implicated persons with pertinent knowledge of some circumstances or aspect of the record subject; such persons may include witnesses or associates of record subjects.

Categories of records in the system:

Records may contain any information, including but not limited to personal identification which may assist the National Drug Intelligence Center (NDIC) in fulfilling its responsibilities to collect, consolidate, analyze, and coordinate multi-source drug intelligence data from all national security and law enforcement agencies; to produce information regarding the structure, finances, communications and activities of drug trafficking organizations and their memberships; and to make such information available, as appropriate, to domestic and law enforcement agencies and to agencies of the U.S. foreign intelligence community. Information will include any data that may assist law enforcement agencies and agencies of the U.S. foreign intelligence community in executing their responsibilities with respect to counterdrug enforcement, including identification, location, arrest and prosecution of persons for narcotics trafficking and related activities and civil proceedings related to such enforcement activities. Such information may be derived from investigative and intelligence reports prepared by law enforcement agencies and agencies of the U.S. foreign intelligence community, documents or other record media seized by law enforcement agencies and made available to NDIC for exploitation, and publicly available information such as media reports and commercially acquired data bases. Records may also include information on persons not implicated in narcotics trafficking or related activities, but with pertinent knowledge of the circumstances of a case or record subject. Such records may contain any information, including but not limited to personal identification data, which may assist NDIC in discharging its responsibilities generally, e.g., information which may assist in identifying and locating persons.

Authority for maintenance of the system:

Sec. 9078, Pub. L. 102-396.

Purpose(s):

This system of records will allow the NDIC to collect and consolidate information from many sources, including law enforcement agencies and agencies of the U.S. foreign intelligence community, in order to be able to produce a more complete picture of the activities of drug trafficking organizations and their memberships than any one such agency can produce on its own. The system will enable NDIC to provide the results of its analyses and other relevant information acquired by it, to Federal, State, and local law enforcement and regulatory agencies, to certain foreign law enforcement agencies, and to agencies of the U.S. foreign intelligence community, to assist them in fulfilling their responsibilities with respect to

enforcement of law related to drug trafficking, including civil proceedings related to enforcement of such laws.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant information contained in this system of records may be disclosed as follows:

1. To the appropriate Federal, State, local, or foreign agency responsible for investigating, enforcing, or implementing a statute, rule, regulation, or order, to the extent that the information is relevant to the recipient's law enforcement function.
2. To the Department of Defense, and components thereof, to support its role in the detection and monitoring of the transportation of illegal drugs into the United States or such other in support of counterdrug law enforcement as may be permitted by law.
3. To individuals or organizations, including Federal, State, local or foreign agencies, in course of counterdrug law enforcement efforts, to the extent necessary to elicit information pertinent to counterdrug law enforcement.
4. To the news media, to the extent releasable in accordance with 28 CFR 50.2, and provided that in each case, that release of the specific information in that situation would not constitute an unwarranted invasion of personal privacy.
5. To the Department of State, and to agencies of the U.S. foreign intelligence community, to further the efforts of those agencies with respect to the national security and foreign affairs aspects of international drug trafficking.
6. To Members of Congress, or their staffs acting upon the Members' behalf, when they request the information on behalf of and at the request of the individuals who are the subjects of the respective records.
7. To the National Archives and Records Administration and the General Services Administration in records management inspections conducted under the authority of 44 CFR 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose

relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are stored on computer at NDIC's headquarters in Johnstown, Pennsylvania and are retrieved both there and at NDIC's Washington area office. Some information, including investigative files and information incorporated into analytical products, may be retained in hard copy format in file folders.

Retrievability:

Access to individual records is gained by use of data retrieval capabilities of computer systems acquired and developed for processing of information in the NDIC Data Base. Data will be retrieved through a number of criteria, including personal identifying information such as name, date of birth, and social security number.

Safeguards:

The NDIC Data Base is protected by both physical security methods and dissemination controls. Fundamental in all cases is that all access to information is limited by a system of password and access control to those NDIC personnel or representatives of other agencies with a demonstrated and lawful need to know the information in order to perform assigned functions. All NDIC personnel capable of accessing the NDIC Data Base will have successfully passed a background investigation, and access by such persons will be limited to those having a "need to know." All accesses to the data base, both internal and external, will be electronically recorded, and such records will be reviewed periodically to ensure against inappropriate access. The NDIC Data Base will be retained within a 24-hour guarded facility which is secured by intruder alarms and other appropriate physical security devices.

Retention and disposal:

A schedule for the retention and disposal of these records is under review and develop

System manager(s) and address:

Director, National Drug Intelligence Center, 319 Washington Street, 5th Floor, Johnstown 15907.

Notification procedures

Inquires should be addressed to: Chief, Administration Branch, National Drug Intelligence Center, 319 Washington Street, 5th Floor, Johnstown, PA 15907.

Record access procedures:

Same as above.

Contesting record procedures

Same as above.

Record source categories:

Information provided by Federal, State, local and foreign law enforcement agencies; agencies of the U.S. foreign intelligence community; and open sources, such as broadcast and print media and publicly available data bases.

Systems exempted from certain provisions of the act

The Attorney General has exempted this system from subsections (c)(3) and (4); (d); (e) and (3); (e)(4)(I); (e)(5) and (8); and (g) pursuant to 5 U.S.C. 552a(j)(2). In addition, the Attorney General has exempted the system from subsections (c)(3), (d), (e)(1) and (e)(4) pursuant to 5 U.S.C. 552a(k) (1) and (2). Rules have been promulgated in accordance with requirements of 5 U.S.C. 553 (b), (c), and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

Office of the Attorney General

JUSTICE/OAG-001

System name:

General Files System of the Office of the Attorney General.

System location:

Office of the Attorney General, United States Department of Justice, 10th and Constitution Avenue NW, Washington, DC 20530.

Categories of individuals covered by the system:

The system encompasses individuals who relate to official Federal investigations, policy decisions, and administrative matters of such significance that the Attorney General maintains information indexed to the name of that individual including, but not limited to, subjects of litigation, targets of investigations, Members and staff members of Congress, upper-echelon government officials, and individuals of national prominence or notoriety.

Categories of records in the system:

Records may include case files, litigation materials, exhibits, internal memoranda or reports, and other records on a given subject or individual. Records vary in number and kind according to the breadth of the Attorney General's responsibilities (28 CFR 0.05) and are limited to those records which are of such significance that the Attorney General has investigative, policy, law enforcement, or administrative interest. An index to these records is described under the caption "Retrievability."

Authority for maintenance of the system:

These records are maintained pursuant to 5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records may be disclosed to the news media and the public pursuant to 28 CFR 17.101 unless it is determined that release of the specific information in the context of a particular

would constitute an unwarranted invasion of privacy.

These records may be disclosed to a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information for investigative or policy decisionmaking purposes or to provide constituent assistance.

These records may be disclosed to members of the judicial branch of the Federal Government in response to a specific request where disclosure appears relevant to the authorized functions of the recipient judicial office or court system.

These records may be disclosed to any civil or criminal law enforcement authorities, whether Federal, State, local or foreign, which require information relevant to a civil or criminal investigation.

These records may be disclosed to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

These records may be disclosed to officials and employees of the White House or any Federal agency which requires information relevant to an agency decision concerning the hiring, appointment, or retention of an employee, the issuance of a security clearance, the conduct of a security or suitability investigation, the classifying of a job, or the issuance of a grant or benefit.

These records may be disclosed to Federal, State, and local licensing agencies or associations which require information concerning the eligibility or suitability of an individual for a license or permit.

These records may be disclosed in a proceeding before a court or adjudicative body before which the Office of the Associate Attorney General is authorized to appear when (a) the Office of the Attorney General, or any subdivision thereof, or (b) any employee of the Office of the Attorney General in his or her official capacity, or (c) any employee of the Office of the Associate Attorney General in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (d) the United States, where the Office of the Attorney General determines that the litigation is likely to affect it or any of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the Office of the Attorney General to be relevant to the litigation.

General to be arguably relevant to the litigation.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Records are stored in paper folders and on index cards. As of May 1982, the index records are also stored on magnetic disks.

Retrievability:

Records created before 1975 are indexed and retrieved manually by subject title. Records created since 1975 are indexed and retrieved manually by subject title, individual's name, Department component which created the record, and by name of the Attorney General whose administration the records were created. As of May 1982 records may also be retrieved through a computerized indexing system.

Safeguards:

Records are maintained in locked cabinets stored in a locked room or, in the case of the records that are classified, in safes or vaults stored in a locked room. The computer is also maintained in a locked room. The computer has a key lock and may be accessed only by persons with a Top Secret clearance by use of a code.

Retention and disposal:

Records are kept indefinitely.

System manager(s) and address:

Special Assistant to the Attorney General, Office of the Attorney General, United States Department of Justice, 10th and Constitution Avenue NW, Washington, DC 20530.

Notification procedure:

Address all inquiries to the system manager. These records will be exempted from subsections (c) (3) and (4); (d); (e) (1), (2) and (3), (e)(4) (G) and (H), (e)(5); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5).

Record access procedures:

Make all requests for access to records from this system in writing to the system manager. Clearly mark both the letter and the envelope "Privacy Act Request."

Contesting record procedures:

Make all requests to contest or amend information maintained in the system in writing to the system manager. State clearly and concisely what information is being contested, the reason for contesting it, and the proposed amendment(s) to the information.

Record source categories:

Sources of information contained in this system include individuals, State, local and foreign government agencies as appropriate, the executive and legislative branches of the Federal Government, and interested third parties.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c) (3) and (4); (d); (e) (2), and (3), (e)(4) (G) and (H), (e)(5); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register*.

These exemptions apply only to the extent that information in a record pertaining to a particular individual relates to official Federal investigations and law enforcement matters. Those f

indexed under an individual's name which concern policy formulation or administrative r
are not being exempted pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) or (k)(5).

[\[TOP\]](#)

Office of the Associate Attorney General

JUSTICE/ASG-001

System name:

General Files System of the Office of the Associate Attorney General, JUSTICE/ASG-001

Security classification:

Not classified.

System location:

Office of the Associate Attorney General, United States Department of Justice, 950
Pennsylvania Avenue, NW., Washington, DC 20530-0001.

Categories of individuals covered by the system:

The system encompasses individuals who relate to official federal investigations, policy decisions, and administrative matters of such significance that the Associate Attorney General maintains information indexed to the name of that individual including, but not limited to subjects of litigation, targets of investigations, Members and staff members of Congress, upper-echelon government officials, and individuals of national prominence or notoriety.

Categories of records in the system:

Records may include case files, litigation materials, exhibits, internal memoranda or reports, and other records on a given subject or individual. Records vary in number and kind according to the breadth of the Associate Attorney General's responsibilities (28 CFR 0.19) and are limited to those which are of such significance that the Associate Attorney General has investigative, policy, law enforcement, or administrative interest.

Authority for maintenance of the system:

These records are maintained pursuant to 5 U.S.C. 301.

Purpose(s):

This system is maintained for the purpose of assisting the Associate Attorney General in carrying out the responsibilities of the Office such as, but not limited to, advising the Attorney General and Deputy Attorney General in formulating Departmental policies and programs, providing overall supervision to organizational units as assigned, and other duties as assigned by the Attorney General (28 CFR 0.19).

Routine uses of records maintained in the system, including categories of users and purpose of such uses:

Information may be disclosed from this system as follows:

A. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

B. To a Member of Congress or staff acting on the Member's behalf when the Member requests the information on behalf of, and at the request of, the individual who is the subject of the record.

C. Law enforcement records may be disclosed to any civil or criminal law enforcement authorities, whether federal, state, local, foreign, or tribal, which require information relevant to a civil or criminal investigation.

D. Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, foreign, or tribal, law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.

E. To the National Archives and Records Administration (NARA) in records management

inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit.

G. To federal, state, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

H. In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator holds the records to be relevant to the proceeding.

I. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

J. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

K. The Department of Justice may disclose relevant and necessary information to a former employee of the Department for the purposes of: Responding to an official inquiry by a state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee if necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

L. To such recipients and under such circumstances and procedures as are mandated by a federal statute or treaty.

Disclosure to consumer reporting agencies:

Not applicable.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:***Storage:***

Records in this system are stored in electronic form and on paper. Records that contain national security information and are classified are stored in accordance with applicable executive orders, statutes, and agency implementing regulations.

Retrievability:

Information can be retrieved by correspondence control number; name of individual; subject matter of topic; or in some cases, by other identifying search term employed.

Safeguards:

Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including the Department's automated systems security and access policies. Classified information is appropriately stored in safes and in accordance with other applicable requirements. In general, records and technical equipment are maintained in buildings with restricted access. The required use of password protection identification features and other system protection methods also restrict access. Access is limited to those officers and employees of the agency who have an official need for access in order to perform their duties.

Retention and disposal:

Records are retained and disposed of in accordance with guidelines approved by the National Archives and Records Administration.

System manager(s) and address:

Deputy Associate Attorney General, Office of the Associate Attorney General, United States Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001.

Notification procedure:

Address inquiries to the System Manager named above.

Record access procedures:

Requests for access should be directed in writing or in person to the System Manager r above. When requests are in writing, the envelope and letter should be clearly marked "Act Access Request." The request should include a general description of the records s and must include the requester's full name, current address, and date and place of birt request must be signed, dated and either notarized or submitted under penalty of perju Some information may be exempt from access provisions as described in the section en "EXEMPTIONS CLAIMED FOR THE SYSTEM." An individual who is the subject of a rec this system may access those records that are not exempt from disclosure. A determina whether a record may be accessed will be made at the time a request is received. Altho specific form is required, you may obtain forms for this purpose from the FOIA/PA Mail F Unit, Justice Management Division, United States Department of Justice, 950 Pennsylv Avenue, NW., Washington, DC 20530-0001, or on the Department of Justice Web site : <http://www.usdoj.gov/04foia/att—d.htm>.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should di their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendrr the information sought. Some information is not subject to amendment, such as tax retu information. Some information may be exempt from contesting record procedures as de in the section entitled "Exemptions Claimed for the System." An individual who is the su a record in this system may amend those records that are not exempt. A determination a record may be amended will be made at the time a request is received.

Record source categories:

Sources of information contained in this system include individuals, state, local, tribal, a foreign government agencies, as appropriate, the executive and legislative branches of Federal Government, the Judiciary, and interested third parties.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d); (e) (3), and (5); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (e) and have been published in the *Federal Register* and at 28 CFR 16.72. These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5). A determination as to exemption shall be made at the time a request for access or amendment is received.

[\[TOP\]](#)

Office of the Deputy Attorney General

JUSTICE/DAG-003

System name:

Drug Enforcement Task Force Evaluation and Reporting System of the Office of the Associate Attorney General.

System location:

Office of the Associate Attorney General, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

The system encompasses individuals who are the subjects of official Federal investigations of the drug task force.

Categories of records in the system:

Records consist of case initiation and indictment records, and monthly reporting and sentencing forms regarding potential or actual targets of investigation of the drug task force.

Authority for maintenance of the system:

These records are maintained pursuant to 5 U.S.C. 301 and 21 U.S.C. 841.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records may be disclosed to the news media and the public pursuant to 28 CFR unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of privacy.

These records may be disclosed to a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information for investigative or policymaking purposes or to provide constituent assistance.

These records may be disclosed to members of the judicial branch of the Federal Government in response to a specific request where disclosure appears relevant to the authorized functions of the recipient judicial office or court system.

These records may be disclosed to any civil or criminal law enforcement authorities, whether Federal, State, local, or foreign, which require information relevant to a civil or criminal investigation.

These records may be disclosed to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

These records may be disclosed to Federal, State, and local licensing agencies or associations which require information concerning the eligibility or suitability of an individual for a license or permit.

These records may be disclosed in a proceeding before a court or adjudicative body before which the Office of the Associate Attorney General is authorized to appear when (a) the Office of the Associate Attorney General, or any subdivision thereof, or (b) any employee of the Office of the Associate Attorney General in his or her official capacity, or (c) any employee of the Office of the Associate Attorney General in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (d) the United States, where the Office of the Associate Attorney General determines that litigation is likely to affect it or any of its

subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the Office of the Associate Attorney General to be arguably relevant to the litigation.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

All records are stored in paper folders. All records, with the exception of indictment forms, are stored also on magnetic disks.

Retrievability:

Records are generally retrieved by case number. Records may be retrieved by individual or name of criminal organization.

Safeguards:

Paper folders are stored in a combination safe which is inside a locked room. This room is part of a locked suite of offices. The magnetic disks and computer are located in the same room. The computer has a key lock. Only those persons with a Top Secret clearance may actually access the computer by using a code.

Retention and disposal:

Records are kept indefinitely.

System manager(s) and address:

Staff Director, Drug Enforcement Task Force, Office of the Associate Attorney General,
and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Address all inquiries to the system manager. These records will be exempted from subsections (c) (3) and (4); (d); (e) (1), (2) and (3), (e)(4) (G) and (H), (e)(5); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

Record access procedures:

None.

Contesting record procedures:

None.

Record source categories:

Sources of information contained in this system include Federal, State, and local government agencies as appropriate, informants, and interested third parties.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c) (3) and (4); (d); (e) (2) and (3), (e)(4) (G) and (H), (e)(5); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DAG-006

System name:

Presidential Appointee Candidate Records System.

System location:

Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

This system encompasses all individuals who are brought to the attention of the Department of Justice as potential candidates for appointment as United States Judges, United States Attorneys, or United States Marshals.

Categories of records in the system:

As to any particular individual, the number and kind of records may vary according to the qualifications of the individual. Thus, these records, in some instances, contain merely letters from the individual himself or some other person recommending his consideration for one of the positions mentioned in the Categories of individuals. The records may also contain biographical sketches of the individual supplied either by the individual himself or the person recommending him. If the individual is under serious consideration for nomination for appointment, a confidential evaluation of his qualifications for the position will be in his folder. Also present may be completed background investigations on the individual. Letters, if any, received, protesting the individual's potential appointment may also be in the folder. Also present would be any information supplied by the individual or any other letters of recommendation.

Authority for maintenance of the system:

These records are maintained pursuant to 5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The routine uses of these records vary with the amount of consideration given to nominating the individual for appointment. In some instances, the records are stored, reviewed by Department personnel, and destroyed as outlined under Retention and Disposal. The candidate's entire record folder would be sent to the President upon his request. After a candidate is nominated and his nomination is pending Senate confirmation, the background

investigation is routinely provided to Chairman of the Senate Judiciary Committee. The fact that the candidate was being considered for appointment would be made known to the referent supplied by the candidate and others contacted. Information about the candidate, as then known, might be supplied to contacted individuals as necessary to verify already obtained information or to seek elaboration of that information.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration. A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Release of information to civil or criminal law enforcement agencies: Information may be disclosed to any civil or criminal law enforcement agency, whether Federal, State, local, or foreign, which requires information relevant to a civil or criminal investigation.

Release of information to agencies regarding the hiring or retention of employees: Information may be disclosed to officials and employees of the White House or any Federal agency which requires information relevant to an agency decision concerning the hiring, appointment, retention of an employee; the issuance of a security clearance; the execution of a security suitability investigation; the classification of a job; or the issuance of a grant or benefit.

Release of information to Federal, State, and local licensing agencies: Information may be disclosed to Federal, State, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

Release of information before a court or adjudicative body: Information may be disclosed in a proceeding before a court or adjudicative body before which the Office of the Deputy Attorney General (ODAG) is authorized to appear when (a) ODAG, or any subdivision thereof, or employee of ODAG in his or her official capacity, or (c) any employee of ODAG in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (d) the United States, where ODAG determines that the litigation is likely to affect it or a subdivision, is a party to litigation or has an interest in litigation and such records are determined by ODAG to be arguably relevant to the litigation.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

These records are maintained in paper folders.

Retrievability:

Information is retrieved from this system by reference first to the office, indexed geographically by the circuit or district, for which the individual is being considered, and then alphabetically by name of the candidate.

Safeguards:

These records are stored in cabinets which are kept in a locked room.

Retention and disposal:

These records are kept for five years and then destroyed, unless the individual receives

appointment. In that event, his individual record is transferred to another records system

System manager(s) and address:

Associate Deputy Attorney General, Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue NW, Washington, DC 20530.

Notification procedure:

Address all inquiries to the System Manager. These records will be exempted from subsections (d)(1) and (e)(1) of section 552a, Title, United States Code, by the Attorney General under the authority of 5 U.S.C. 552a(k)(5) to the extent therein permitted.

Record access procedures:

A request for access to non-exempt portions of records from this system should be directed orally or in writing to the Associate Deputy Attorney General. When requests are in writing, the envelope and letter should clearly be marked "Privacy Access Request."

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the Associate Deputy Attorney General stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information.

Record source categories:

Non-exempt sources of information in this system include the general public, the candidates themselves, government agencies where appropriate, and any other interested party.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (d)(1) and (e)(1) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DAG-007

System name:

Presidential Appointee Records System.

System location:

Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue NW, Washington, DC 20530.

Categories of individuals covered by the system:

The system encompasses the following: Department of Justice Presidential appointees retired, resigned, or deceased appointees.

Categories of records in the system:

This system of records consists of records folders which may contain up to five sections. The personnel section includes such items as biographical sketches, qualification statement completed Civil Service forms if applicable, letters recommending appointment, notification of appointment, and other personnel-related matters. The character section contains complete or portions of ongoing background investigations and matters related thereto. The Congressional section contains Congressional and other political type recommendations regarding appointment. The protest section contains correspondence, if any exists, protesting the appointment of candidates. The complaint section contains correspondence from individuals or groups complaining about office holders.

Authority for maintenance of the system:

These records are maintained pursuant to 5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Generally, these records are used only for internal Department of Justice purposes. Prior appointment, routine uses would include those specified for the Presidential Appointee Candidate Records System. If an appointee leaves the Department, information contained in his personnel folder might be used as the basis for answering inquiries from prospective employers about his qualifications and performance. The personnel section of his folder might be made available to other federal agencies, at their request, upon the transfer of the appointee to such an agency.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specified information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Release of information to civil or criminal law enforcement agencies: Information may be disclosed to any civil or criminal law enforcement agency, whether Federal, State, local, or foreign, which requires information relevant to a civil or criminal investigation.

Release of information to agencies regarding the hiring or retention of employees: Information may be disclosed to officials and employees of the White House or any Federal agency which requires information relevant to an agency decision concerning the hiring, appointment, retention of an employee; the issuance of a security clearance; the execution of a security suitability investigation; the classification of a job; or the issuance of a grant or benefit.

Release of information to Federal, State, and local licensing agencies: Information may

disclosed to Federal, State, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

Release of information before a court or adjudicative body: Information may be disclosed in a proceeding before a court or adjudicative body before which the Office of the Deputy Attorney General (ODAG) is authorized to appear when (a) ODAG, or any subdivision thereof, or employee of ODAG in his or her official capacity, or (c) any employee of ODAG in his or her individual capacity where the Department of Justice has agreed to represent the employee, (d) the United States, where ODAG determines that the litigation is likely to affect it or any subdivisions, is a party to litigation or has an interest in litigation and such records are determined by ODAG to be arguably relevant to the litigation.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

These records are stored in paper folders.

Retrievability:

Information is retrieved by using the name of the individual who is the subject of the folder.

Safeguards:

These records are stored in cabinets which are kept in a locked room.

Retention and disposal:

The personnel section of these records is retained indefinitely at the Office of the Deputy Attorney General, except in the instance of an appointee who resigns or dies, in which case that section is sent to the St. Louis Records Center for indefinite storage. All other sections of the folders, in the instance where an appointee dies or resigns, are sent to the Suitland Maryland Records Center for storage for five years and then destroyed.

System manager(s) and address:

Associate Deputy Attorney General, Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Address all inquiries to the System Manager. These records will be exempted from subsections (d)(1) and (e)(1) of section 552a, Title 5, United States Code, by the Attorney General under the authority of 5 U.S.C. 552a(k)(5) to the extent therein permitted.

Record access procedures:

A request for access to non-exempt portions of records from this system should be directed orally or in writing to the System Manager. When requests are in writing, the envelope or letter should clearly be marked "Privacy Access Request."

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager, stating clearly and concisely what information is being contested the reasons for contesting it, and the proposed amendment(s) to the information.

Record source categories:

Non-exempt sources of information contained in this system include the general public, subjects of the records themselves, government agencies when appropriate, and any other interested party.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (b)(1) and (e)(1) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DAG-008

System name:

Special Candidates for Presidential Appointments and Noncareer SES Positions Record System.

System location:

Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

The system encompasses all individuals under consideration for presidential appointments, division heads, deputy division heads, or noncareer SES positions in the Department of Justice.

Categories of records in the system:

The system of records consists of personnel folders which may contain up to a total of five sections. The personnel section contains records such as résumés, letters of recommendation, and related personnel matters. The character section contains complete and portions of ongoing background investigations and matters related thereto. The Congressional section contains Congressional and other political type recommendations regarding appointment. The protest section contains correspondence, if any exists, protesting the appointment of candidates. The majority of these personnel folders contain only the personnel section.

Authority for maintenance of the system:

These records are maintained pursuant to 5 U.S.C. 301.

Purpose(s):

Records are maintained in this system to assist the President, White House officials or employees, the Congress, and/or Department of Justice officials in obtaining information necessary to determine the qualifications and suitability of candidates for the positions of Department of Justice division head, deputy division head or noncareer SES.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Relevant information from this system may be disclosed as indicated below: The routine uses of these records vary with the amount of consideration given to nominating, clearing or selecting the candidate for appointment. In some instances, the records are stored, reviewed by designated Department personnel, and destroyed as outlined under Retention and Disposal. The candidate's record folder, or a portion thereof, may be provided to the White House. The fact that the candidate was being considered for appointment would be made known to the references supplied by the candidate and others contacted. Information about the candidate, as then known, might be supplied to such references and/or such contacted individuals as necessary to verify already obtained information or to seek elaboration of information.

Information permitted to be released to the news media and the public pursuant to 28 C.F.R. 50.2 may be made available unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Information not otherwise required to be released pursuant to 5 U.S.C. 552 may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is subject of the record.

A record from this system of records may be disclosed as a routine use to the General Services Administration and the National Archives and Records Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

In the event that a record(s) in this system indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, or foreign agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing su

Information may be disclosed to officials and employees of the White House or any Fed agency which requires information relevant to an agency decision concerning the hiring appointment, or retention of an employee; the issuance of a security clearance; the exe of a security or suitability investigation; the classification of a job; or the issuance of a gr benefit.

Information may be disclosed to Federal, State, and local licensing agencies or associa which require information concerning the suitability or eligibility of an individual for a lice permit.

Information may be disclosed in a proceeding before a court or adjudicative body before the Office of the Deputy Attorney General (ODAG) is authorized to appear when (a) OD any subdivision thereof, or (b) any employee of ODAG in his or her official capacity, or (employee of ODAG in his or her individual capacity where the Department of Justice ha agreed to represent the employee, or (d) the United States, where ODAG determines th litigation is likely to affect it or any of its subdivisions, is a party to litigation or has an int litigation and such record is determined by ODAG to be arguably relevant to the litigatio

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or profess licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related o official purposes where the Department requires information and/or consultation assista from the former employee regarding a matter within that person's former area of respon

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

These records are stored in paper holders.

Retrievability:

Information is retrieved by the name of individuals seeking appointment as the files are arranged alphabetically by same.

Safeguards:

These records are in cabinets in a locked room.

Retention and disposal:

In the event a candidate is not nominated or selected for appointment, his record is maintained for five years and then destroyed. If the candidate is appointed, his records are transferred to the Presidential Appointee Records System.

System manager(s) and address:

Associate Deputy Attorney General, Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue NW, Washington, DC 20530.

Notification procedure:

Address all inquiries to the System Manager. These records will be exempted from subsections (d)(1) and (e)(1) of sections 552a, title 5, United States Code, by the Attorney General under the authority of 5 U.S.C. 552a(k)(5) to the extent therein permitted.

Record access procedure:

A request for access to non-exempt portions of records from this system should be directed orally or in writing to the System Manager. When requests are in writing, the envelope and letter should clearly be marked "Privacy Access Request."

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct

their request to the System Manager, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment(s) to the information.

Record source categories:

Sources of information include the general public, the subjects of the records themselves, government agencies when appropriate, and parties who know the record subject.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (d)(1) and (e)(1) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5). Rules have been promulgated in accordance with the requirement of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DAG-009

System name:

Summer Intern Program Records System.

System location:

Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

All individuals who submit applications for the Department's Summer Intern Program for Students.

Categories of records in the system:

The system of records consists of items such as completed Civil Service forms, law school grade transcripts, letters of recommendation, and completed Summer Law Intern Applications.

Authority for maintenance of the system:

These records are maintained pursuant to 5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records are used by Department personnel for recruitment purposes. However, in case of an applicant with regard to whom the Department has decided not to extend an employment, his or her application and Civil Service forms might be referred to another agency, upon its request, for that agency's recruitment purposes.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Department's behalf of and at the request of the individual who is the subject of the records.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 5 U.S.C. 2904 and 2906.

Release of information to civil or criminal law enforcement agencies: Information may be disclosed to any civil or criminal law enforcement agency, whether Federal, State, local, or foreign, which requires information relevant to a civil or criminal investigation.

Release of information to agencies regarding the hiring or retention of employees: Information may be disclosed to officials and employees of the White House or any Federal agency which requires information relevant to an agency decision concerning the hiring, appointment, retention of an employee; the issuance of a security clearance; the execution of a security

suitability investigation; the classification of a job; or the issuance of a grant or benefit.

Release of information to Federal, State, and local licensing agencies: Information may be disclosed to Federal, State, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

Release of information before a court or adjudicative body: Information may be disclosed in a proceeding before a court or adjudicative body before which the Office of the Deputy Attorney General (ODAG) is authorized to appear when (a) ODAG, or any subdivision thereof, or any employee of ODAG in his or her official capacity, or (c) any employee of ODAG in his or her individual capacity where the Department of Justice has agreed to represent the employee, (d) the United States, where ODAG determines that the litigation is likely to affect it or any of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by ODAG to be arguably relevant to the litigation.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

These records are stapled together.

Retrievability:

Information is retrieved by use of the applicant's name, as these records are filed by use of the first letter of the applicant's last name.

Safeguards:

These records are maintained in cabinets stored in a locked room.

Retention and disposal:

These records are retained, in the case of applicants who are not offered positions, for 6 months and then destroyed. In the case of accepted applicants, their records enter the Civil Service system.

System manager(s) and address:

Associate Deputy Attorney General, Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Same as the above.

Record access procedures:

A request for access to these records should be directed orally or in writing to the System Manager. When requests are in writing, the envelope and letter should clearly be marked 'Privacy Access Request'.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment(s) to the information.

Record source categories:

Information contained in this system is obtained from the applicant and references provided by him.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/DAG-010

System name:

United States Judge and Department of Justice Presidential Appointee Records.

System location:

Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

This system encompasses all United States Judges and all Department of Justice Presidential Appointees.

Categories of records in the system:

- A. 1. Card index relating to United States Judges which includes name, salary, Congressional appointment, State of birth, political party (if voluntarily provided), religion (if voluntarily provided), and American Bar Association rating.
- 2. Information on the above mentioned card index, except religion, is also maintained on processing equipment.
- B. Cross index of judges' names and districts.
- C. Roster of districts showing the dates of duty of district court judges and Department of Justice Presidential Appointees, indexed alphabetically by name.
- D. Book of commissions of United States Judges and Department of Justice Presidential Appointees in order by date of appointment and indexed alphabetically by name.
- E. Nomination book showing the name of the nominated Judge or Department of Justice Presidential Appointee.

Presidential Appointee, the date the proposed nomination was sent to the White House date the nomination was made to the Senate, the date of confirmation, the date of appointment, and the date of entrance on duty. This book is in chronological order, and indexed alphabetically by name of the nominee.

Authority for maintenance of the system:

These records are maintained pursuant to 5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records are maintained to make responses to public inquiries regarding these individuals noted in Categories of individuals (the political party and religion of an appointee not released), and for Department internal purposes.

Release of information to the new media: Information permitted to be released to the new media and the public pursuant to 28 CFR 50.2 may be made available from system of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Release of information to civil or criminal law enforcement agencies: Information may be disclosed to any civil or criminal law enforcement agency, whether Federal, State, local, foreign, which requires information relevant to a civil or criminal investigation.

Release of information to agencies regarding the hiring or retention of employees: Information may be disclosed to officials and employees of the White House or any Federal agency requires information relevant to an agency decision concerning the hiring, appointment, retention of an employee; the issuance of a security clearance; the execution of a security suitability investigation; the classification of a job; or the issuance of a grant or benefit.

Release of information to Federal, State, and local licensing agencies: Information may be disclosed to Federal, State, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

Release of information before a court or adjudicative body: Information may be disclosed in a proceeding before a court or adjudicative body before which the Office of the Deputy Attorney General (ODAG) is authorized to appear when (a) ODAG, or any subdivision thereof, or employee of ODAG in his or her official capacity, or (c) any employee of ODAG in his or her individual capacity where the Department of Justice has agreed to represent the employee, (d) the United States, where ODAG determines that the litigation is likely to affect it or a subdivision, is a party to litigation or has an interest in litigation and such records are determined by ODAG to be arguably relevant to the litigation.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

These records are kept on cards, in folders, in books, or on diskettes.

Retrievability:

Information is retrieved by those data elements identified in the "Categories of Records

System" section of this notice.

Safeguards:

Biological sketches and diskettes are kept in a locked safe. All other information is kept in cabinets or card files.

Retention and disposal:

This information is maintained indefinitely.

System manager(s) and address:

Associate Deputy Attorney General, Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Same as the above.

Record access procedures:

A request of access to these records should be directed orally or in writing to the System Manager. When requests are in writing the envelope and letter should clearly be marked "Privacy Access Request."

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment(s) to the information.

Record source categories:

Information contained in this system is obtained from the individuals who are the subjects of the records and from other Department of Justice records.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/DAG-011

System name:

Miscellaneous Attorney Personnel Records System.

System location:

Office of the Deputy Attorney General United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

Persons who applied to or are employed by the Department of Justice as attorneys and included within another OAAG system.

Categories of records in the system:

This system of records consists of records folders which may contain up to a total of four sections. The personnel section contains records such as resumes, letter of recommendation, law school grade transcripts, completed Civil Service forms, and related personnel matters. The character section contains completed or portions of ongoing background investigations and matters related thereto. The Congressional section contains Congressional and other political type recommendations regarding appointment. The protest section contains correspondence, if any exists, protesting the appointment of applicants. The complaint section contains correspondence from individuals or groups complaining about office holders and contain matters relating to the disposition of those complaints. Rarely does a personnel folder contain more than the personnel and character sections.

Authority for maintenance of the system:

The records are maintained pursuant to 5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records are used only by Department of Justice personnel. Information contained in a folder may be used as the basis for answering future inquiries from other government agencies about a former employee's qualifications. The personnel section may be made available to other federal agencies, at their request, upon the transfer of an employee to such an agency.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 5 U.S.C. 2904 and 2906.

Release of information to civil or criminal law enforcement agencies: Information may be disclosed to any civil or criminal law enforcement agency, whether Federal, State, local, or foreign, which requires information relevant to a civil or criminal investigation.

Release of information to agencies regarding the hiring or retention of employees: Information may be disclosed to officials and employees of the White House or any Federal agency which requires information relevant to an agency decision concerning the hiring, appointment, retention of an employee; the issuance of a security clearance; the execution of a security suitability investigation; the classification of a job; or the issuance of a grant or benefit.

Release of information to Federal, State, and local licensing agencies: Information may be disclosed to Federal, State, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

Release of information before a court or adjudicative body: Information may be disclosed in a proceeding before a court or adjudicative body before which the Office of the Deputy Attorney General (ODAG) is authorized to appear when (a) ODAG, or any subdivision thereof, or any employee of ODAG in his or her official capacity, or (c) any employee of ODAG in his or her individual capacity where the Department of Justice has agreed to represent the employee, (d) the United States, where ODAG determines that the litigation is likely to affect it or any of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by ODAG to be arguably relevant to the litigation.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

These records are stored in paper folders.

Retrievability:

Information is retrieved by use of an individual's name, as the folders are filed alphabetically by name.

Safeguards:

These records are maintained in cabinets stored in a lockable room.

Retention and disposal:

These records are retained until the subjects of the files resign or otherwise leave their employment for non-federal employment. In that instance, the personnel section is sent to the St. Louis Records Center for an indefinite period. If the individual transfers to another agency of the Federal government, the personnel section is sent to the gaining agency. All other sections of the folder are destroyed six months after the individual leaves office. The entire folders of individuals who were applicants and were not offered employment or did not accept employment with the Department are destroyed one year after final action is taken on their application.

System manager(s) and address:

Associate Deputy Attorney General, Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Address all inquiries to the System Manager. These records will be exempted from subsections (d)(1) and (e)(1) of section 552a, Title 5, United States Code, by the Attorney General under the authority of 5 U.S.C. 552a(k)(5) to the extent therein permitted.

Record access procedures:

A request for access to non-exempt portions of records from this system should be directed orally or in writing to the System Manager. When requests are in writing, the envelope and letter should clearly be marked "Privacy Access Request."

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment(s) to the information.

Record source categories:

Non-exempt sources of information contained in this system include the individuals who

subjects of the records, government agencies as appropriate, and interested third parties.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (d)(1) and (e)(1) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/DAG-013

System name:

General Files System of the Office of the Deputy Attorney General.

System location:

Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue NW, Washington, DC 20530.

Categories of individuals covered by the system:

The system encompasses individuals who relate to official Federal investigations, policy decisions, and administrative matters of such significance that the Deputy Attorney General maintains information indexed to the name of that individual, including, but not limited to subjects of litigation, targets of investigations, Members and staff members of Congress, upper-echelon government officials, and individuals of national prominence or notoriety.

Categories of records in the system:

Records may include case files, litigation materials, exhibits, internal memoranda and reports or other records on a given subject or individual. Records vary in number and kind according to the breadth of the Deputy Attorney General's responsibilities (28 CFR 0.15) and are limited to those which are of such significance that the Deputy Attorney General has investigative or law enforcement interest, or administrative interest. An index to these records is described under

caption "Retrievability."

Authority for maintenance of the system:

These records are maintained pursuant to 5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records may be disclosed to the news media and the public pursuant to 28 CFR unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of privacy.

These records may be disclosed to a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information for investigative or policy decisionmaking purposes or to provide constituent assistance.

These records may be disclosed to members of the judicial branch of the Federal Government in response to a specific request where disclosure appears relevant to the authorized functions of the recipient judicial office or court system.

These records may be disclosed to any civil or criminal law enforcement authorities, whether Federal, State, local, or foreign, which require information relevant to a civil or criminal investigation.

These records may be disclosed to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

These records may be disclosed to officials and employees of the White House or any Federal agency which requires information relevant to an agency decision concerning the hiring or appointment, or retention of an employee, the issuance of a security clearance, the conduct of a security or suitability investigation, the classifying of a job, or the issuance of a grant or benefit.

These records may be disclosed to Federal, State, and local licensing agencies or associations which require information concerning the eligibility or suitability of an individual for a license.

permit.

These records may be disclosed in a proceeding before a court or adjudicative body before which the Office of the Deputy Attorney General is authorized to appear when (a) the Office of the Deputy Attorney General, or any subdivision thereof, or (b) any employee of the Office of the Deputy Attorney General in his or her official capacity, or (c) any employee of the Office of the Deputy Attorney General in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (d) the United States, where the Office of the Deputy Attorney General determines that the litigation is likely to affect it or any of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the Office of the Deputy Attorney General to be arguably relevant to the litigation.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records are stored in paper folders and on index cards. As of April, 1982, the index records are also stored on magnetic disks.

Retrievability:

Deputy Attorney General records created prior to 1973 were incorporated into Attorney General files, and are retrievable from the index to the General Files System of the Office of the Attorney General. Records created by the Office of the Deputy Attorney General since 1973 are indexed and retrieved manually by use of the subject title, individual's name, or Department component which created the record. As of April 1982, records may also be retrieved through a computerized logging system.

Safeguards:

Records are maintained in locked cabinets stored in a locked room or, in the case of the records that are classified, in safes or vaults stored in a locked room. The computer is maintained in a locked room. The computer has a key lock and may be accessed only by persons with a Top Secret clearance by use of a code.

Retention and disposal:

Records are kept indefinitely.

System manager(s) and address:

Associate Deputy Attorney General, Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Address all inquiries to the system manager. These records will be exempted from subsections (c) (3) and (4); (d); (e) (1), (2), and (3), (e)(4) (G) and (H), (e)(5); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5).

Record access procedures:

Make all requests for access to records from this system in writing to the system manager. Clearly mark both the letter and envelope "Privacy Act Request."

Contesting record procedures:

Make all requests to contest or amend information maintained in the system in writing to the system manager. State clearly and concisely what information is being contested, the reason for contesting it, and the proposed amendment(s) to the information.

Record source categories:

Sources of information contained in this system include individuals, State, local and foreign government agencies as appropriate, the executive and legislative branches of the Federal

Government, and interested third parties.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c) (3) and (4); (d); (e) (2), and (3), (e)(4) (G) and (H), (e)(5); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5). Rules have been promulgated in accordance with the requirement of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register*. These exemptions apply only to the extent that information in a record pertaining to a particular individual relates to official Federal investigations and law enforcement matters. Those records indexed under an individual's name and which concern policy formulation or administrative matters are not being exempted pursuant to 5 U.S.C. 552(j)(2), (k)(1), (k)(2) or (k)(5).

[\[TOP\]](#)

Office of Community Oriented Policing Services

JUSTICE/COPS-001

System name:

Police Corps System, Justice/COPS-001.

System location:

Records may be retained at the U.S. Department of Justice ("DOJ"), Office of Community Oriented Policing Services ("COPS"), Office of the Police Corps and Law Enforcement Education, 1100 Vermont Ave., NW., Washington, DC 20530.

Categories of individuals covered by the system:

Individuals who have applied for educational scholarships under the Police Corps Program; individuals who have been approved to receive such scholarships; and individuals who are receiving, or have received, funds provided under the Police Corps Program.

Categories of records in the system:

Included are any records which may assist COPS in its administration of the Police Corps

Program. Records may include an individual's name; Social Security number; current residence and telephone number; financial data; scholarship application and associated personal, professional and demographic background information (including age, race and gender); educational background and achievements; progress reports; designated police department assignment; and employment record within the assigned police department. Records may also include those generated as a result of a scholarship recipient's failure to serve in a designated agency or otherwise fulfill the terms of the agreement (e.g. amount, status of claim; history of claim; and other records relevant to the scholarship recipient's efforts to fulfill the terms of the agreement).

Authority for maintenance of the system:

This system of records is established and maintained under the authority of 5 U.S.C. 552, 42 U.S.C. 14095, 14097, 14102.

Purpose(s):

The purpose of the Police Corps System of Records is to support COPS in its administration of the Police Corps program which provides educational scholarships to students in exchange for their commitment to serve in a designated police department upon graduation. It will enable COPS to monitor the progress of the Police Corps program and its scholarship recipients, to maintain records on and to verify that all of the scholarship applicants and/or recipients provided accurate background information, to calculate and verify amounts of educational assistance to be awarded, to process scholarship-related payments, and to select the State agencies which will participate in the Police Corps program. It will also allow COPS to manage the collection of debts associated with the granting of scholarships.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

1. Relevant information may be used by Department of Treasury personnel in the processing of scholarship-related payments.
2. Relevant records may be disclosed, as appropriate, to designated State agencies to assist them in recruiting, screening and matching individuals with an appropriate police department.
3. Relevant records may be disclosed to contractors and subcontractors to the extent necessary for the performance of their duties.

necessary to perform the required law enforcement training, administrative tasks, technical installations, maintenance operations and/or other similar duties.

4. In the event that a record(s) indicates a violation or a potential violation of the law, whether civil, criminal or regulatory in nature, the relevant records may be disclosed to the agency charged with enforcing or implementing such law.

5. Relevant records may be disclosed to a court or adjudicative body before which DOJ is authorized to appear when any of the following is a party to the litigation or has an interest in the litigation, and such records are determined by COPS to be arguably relevant to the litigation: (a) COPS or any subdivision thereof; (b) any COPS or other DOJ employee in his or her official capacity; (c) any COPS or other DOJ employee in his or her individual capacity where DOJ has agreed to represent the employee; or (d) the United States, where COPS has determined that the litigation is likely to affect it or any of its subdivisions.

6. Relevant records may be disclosed to an actual or potential party or to his or her attorney for the purpose of negotiation or discussion on such matters as settlement of the case or for use in formal or informal discovery proceedings.

7. Relevant records may be disclosed to a Federal agency in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of any employee, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter.

8. Relevant records may be disclosed to Federal, State, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

9. Relevant records may be disclosed to the National Archives and Records Administration or the General Services Administration for use in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

10. Relevant records may be disclosed to other Federal or State agencies as specified in applicable law or implementing regulations.

11. Relevant records may be disclosed to the news media and the public pursuant to 28

50.2 unless it is determined that the release of the specific information in the context of particular case would constitute an unwarranted invasion of personal privacy.

12. Relevant records may be disclosed to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at request of the individual who is the subject of the record.

13. Relevant records may be disclosed to the Internal Revenue Service to obtain addresses which may be used to locate a scholarship recipient, including delinquent scholarship recipients; or, where appropriate, to obtain information such as will enable COPS to assess and verify the ability of a delinquent scholarship recipient to repay debts owed to the Federal Government, e.g., information as to whether a scholarship applicant has a delinquent tax account, or a tax refund due.

14. Relevant records may be provided to another Federal agency to effect either a salary or an authorized administrative offset to a delinquent account in order to collect debts owed to the Federal Government; or, when other collection efforts have failed, to the IRS to effect offset against Federal income tax refund due, but only after due process requirements have been met.

15. Relevant records may be disclosed to any third party who may possess the information such as the U.S. Post Office, a State motor vehicle administration, a professional organization, an alumni association, etc., to obtain a current mailing address of the scholarship recipient including delinquent scholarship recipients, in order to locate such individual(s).

16. Relevant records may be disclosed to a Federal, State, local, or foreign agency, or to an individual or organization, if there is reason to believe that such agency, individual, or organization possesses information relating to the debt, the identity or location of the debtor, the debtor's ability to pay, or relating to any other matter which is relevant and necessary to the settlement, effective litigation and enforced collection of the debt, or relating to the civil trial or hearing, and the disclosure is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an agency.

17. Addresses obtained from the IRS may be redisclosed as follows:

(a) To debt collection agencies (or agents), but only for the purpose of locating an individual

to collect or compromise a claim;

(b) To consumer reporting agencies as part of the information provided under subsection (b)(12) (described below) which is directly related to the identity of the debtor.

Disclosure to consumer reporting agencies:

In accordance with section 3711(f) of Title 31 (as authorized under subsection (b)(12) of Privacy Act (5 U.S.C. 552a)):

Information may be disclosed to a consumer reporting agency (as defined by 15 U.S.C. 1681a(f) and 31 U.S.C. 3701(a)(3)) where such information is directly related to the identity of the debtor, i.e., name, address, and taxpayer ID (SS#), together with the amount, status, history of claim, and agency or program under which claim arose, for the purpose of encouraging repayment of overdue debts, e.g., to provide an incentive for delinquent scholarship recipients to repay Federal Government debts by making these debts a part of their credit records. Such disclosure may be made only when a claim is overdue and on due process steps have been taken to notify the delinquent recipient and give him or her a chance to meet the terms of the debt. Prior to such disclosure, satisfactory assurances must be obtained from such consumer reporting agency concerning compliance by that agency with the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) and any other Federal law governing provisions of consumer credit information.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information may be stored on electronic media via a configuration of personal computer

servers and mainframes, using hard disks, floppy diskettes, magnetic tape, compact disc and/or optical disks. Documentary records will be maintained in file folders.

Retrievability:

Records will be retrievable by identifying an individual's name; Social Security number; department assignment; educational institution; or other identifying number or character

Safeguards:

Information will be safeguarded in accordance with U.S. Department of Justice rules and policies governing the security and access to automated information systems. These safeguards include the use of passwords and user identification codes to limit access of authorized personnel in the performance of their official duties with respect to the Police program. Additionally, paper records will be stored in secured areas to prevent unauthorized access. Moreover, any individual who has access to the system of records will be required to protect the information from public view and from unauthorized use.

Retention and disposal:

Records will be retained and/or destroyed in accordance with U.S. Department of Justice rules and policies. The retention and destruction schedule for these records is pending approval. Computerized records will be destroyed by shredding, degaussing, etc., and document records will be destroyed by shredding.

System manager(s) and address:

Director, Office of Community Oriented Policing Services, Office of the Police Corps and Enforcement Education, 1100 Vermont Avenue, NW, Washington, DC 20530.

Notification procedure:

Please direct any inquiries concerning the system of records, including questions relating to whether the system contains information about you, to the System Manager identified above.

Record access procedures:

Address requests in writing to the System Manager identified above, and provide a reasonable

description of the record being sought.

Contesting record procedures:

Address requests in writing to the System Manager identified above and provide a reasonable description of the record; state clearly and concisely the information being contested, the reasons for requesting the correction, and the proposed amendment to the information. In addition, provide supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

Record source categories:

All information contained in the system of records is obtained from the individuals covered by the system; their educational institutions; consumer reporting agencies; designated State agencies; other Federal agencies, including but not limited to the IRS and the U.S. Postal Service; and third parties who serve as references for the individual.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

National Security Division

JUSTICE/NSD-001

System Name:

Foreign Intelligence and Counterintelligence Records System.

Security Classification:

The majority of information in this system of records is classified. The remaining information is Sensitive But Unclassified.

System Location:

United States Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530-0001.

Categories of Individuals Covered by the System:

Individuals who are the subject of applications for electronic surveillance, physical search, or other foreign intelligence and foreign counterintelligence investigations authorized by the Foreign Intelligence Surveillance Court (FISC) pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. 1801 *et seq.* (FISA), Executive Order 12958 and other applicable executive orders governing foreign intelligence; individuals about whom information was obtained by a foreign intelligence electronic surveillance or other search; individuals whose issues pertaining to the surveillance or search were raised in subsequent litigation; individuals whose activities are the subject of a properly authorized foreign intelligence, foreign counterintelligence, or international terrorism investigation, or investigative techniques not requiring approval from the FISC or whose activities form the crux of a foreign intelligence or counterintelligence policy or operational question; individuals who are not the subjects or proposed subjects of particular investigations or investigative techniques, but who are included in connection with the authorities for such investigations or techniques, because of their communications or associations with such subjects or their involvement in related activities; individuals of foreign intelligence or counterintelligence (including counterterrorism) interest; and NSA attorneys.

Categories of Records in the System:

The system consists of FISA applications, authorizations for foreign intelligence and foreign counterintelligence operations, supporting documentation, and FISC orders or Attorney General certifications, as appropriate. This includes notes, memoranda, legal opinions, and reports acquired or produced by the National Security Division (NSD) in the course of performing its assigned functions of preparing FISA applications. Included in this system are recommendations to the Attorney General concerning Attorney General authorizations for physical searches, pursuant to Executive Order (E.O.) 12333, and electronic surveillance abroad of United States persons that are requested by entities within the Intelligence Community pursuant to FISA and other applicable executive orders governing foreign intelligence. This system also includes documents related to authority to conduct particular investigations or to use certain techniques in particular investigations. Included in this system are legal opinions regarding questions of law and policy that relate to United States

intelligence activities, and supporting documentation prepared in connection with litigation

Authority for Maintenance of the System:

This system was established and is maintained pursuant to 44 U.S.C. 3101, 3103, 3105 CFR 0.72, to implement the provisions of 50 U.S.C. 1801 *et seq.* as amended and the applicable executive order(s) governing foreign intelligence surveillance and classified national security information.

Purpose of the System:

This system is maintained to enable NSD staff to prepare applications under FISA; maintain an accurate record of applications filed by the United States before the FISC; participate in review, development, implementation and oversight of United States intelligence, counterintelligence, and national security policy matters; provide legal advice to the Attorney General and the United States intelligence agencies regarding questions of law and policy that relate to United States intelligence activities; support litigation issues pertaining to foreign intelligence collections; and, analyze, interpret, and comment upon proposed statutes, executive orders, guidelines and other directives pertaining to foreign intelligence, counterintelligence, and national security activities.

Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses:

These records are routinely used by NSD staff in performing the duties ascribed to the Information. Information may be disclosed from this system consistent with restrictions that apply to classified information, and consistent with the FISA, as follows:

A. To any court, department, officer, agency, regulatory body or other authority of the United States, a state or a political subdivision thereof, or to any aggrieved person or representative of an aggrieved person, during the course of a trial, hearing, or other proceeding.

B. In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding, or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

C. To the Administrative Office of the United States Courts and to Congress.

D. To agencies or entities in the intelligence community that have submitted a policy or operational question to the NSD when the information is necessary in the course of providing legal advice in response to the question.

E. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

F. To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

G. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

H. To a former employee of the Department for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

I. To such recipients and under such circumstances and procedures as are mandated by a federal statute or treaty.

J. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft, fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise.

confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to Consumer Reporting Agencies:

None.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing Records in the System:

Storage:

Records in this system are stored on paper, and/or in electronic form. Records that contain classified national security information are stored in accordance with applicable executive orders, statutes, and agency implementing regulations.

Retrievability:

Information is retrieved by the name of the actual or proposed target of the electronic surveillance or physical search, and persons in contact with the target. Information may be retrieved by the caption of the litigation, including the names of individuals, and through use of a subject matter index that includes the names of individuals. Information may also be retrieved by name of the NSD attorney assigned.

Safeguards:

Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including the Department's automated systems security and access policies. Classified information is appropriately stored in safes and in accordance with other applicable requirements. Records and technical equipment are maintained in a secured area with restricted access. The required use of password protection identification features and other system protection methods also restrict access.

Retention and Disposal:

Records in this system are maintained and disposed of in accordance with all applicable statutory and regulatory requirements.

System Manager and Address:

Deputy Counsel for Intelligence Policy, Office of Intelligence Policy & Review, National Security Division, U.S. Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001.

Notification Procedures:

Address any inquiries to the System Manager listed above.

Record Access Procedures:

A major part of this system is exempted from this requirement under subsections (c)(3) (d); (e)(1), (2), (3), (4)(G), (H) and (I), (5) and (8); (f); (g); and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (2), and (5). A determination as to exemption shall be made each time a request for access is received. A request for access to records contained in this system shall be made in writing, with the envelope and letter clearly marked "Privacy Act Request". The request should include the full name of the individual involved, the individual's current address, date and place of birth, and his or her signature which shall be notarized or made pursuant to 28 U.S.C. 1746 as an unsworn declaration, along with any other information that may be of assistance in locating and identifying the record. The requester will also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

Contesting Record Procedures:

Individuals seeking to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information.

Record Source Categories:

Sources of information contained in this system include applications to the FISC and supporting documents that include investigative reports from federal law enforcement and intelligence agencies and other executive branch departments, and agencies conducting foreign counterintelligence and terrorism investigations that are client agencies of the

Department of Justice. Occasional information from state, local or foreign governments, of criminal, civil and appellate court documents and related material, and the work product of the Department of Justice and federal agency attorneys may also be included within this system.

Exemptions Claimed for the System:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d); (e)(3), (4)(G), (H) and (I), (5) and (8); (f); (g); and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (2), and (5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register*. These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (2) or (5). A determination as to whether an exemption shall be made at the time a request for access or amendment is received.

[\[TOP\]](#)

JUSTICE/NSD-002

SYSTEM NAME:

Registration and Informational Material Files Under the Foreign Agents Registration Act of 1938.

SECURITY CLASSIFICATION:

Sensitive but Unclassified.

SYSTEM LOCATION:

U.S. Department of Justice; National Security Division; 950 Pennsylvania Ave., NW., Washington, DC 20530.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Persons who have registered under the Foreign Agents Registration Act of 1938, as amended (FARA), 22 U.S.C. 611 *et seq.*, and persons referenced in correspondence or other files maintained in connection with FARA.

CATEGORIES OF RECORDS IN THE SYSTEM:

(1) Automated alphabetical indices which include summary data such as registrant name, numbers, dates of registration, and a synopsis of activities performed for a given foreign principal; and (2) file folders which contain copies of all registration statements and statements concerning the distribution of informational materials furnished under FARA.

Other records related to subject matters described in this system may include related correspondence, inspection and/or investigative reports, and/or statements of any agent of a foreign principal whose activities have ceased to be of a character which requires registration under FARA.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

This system is established and maintained pursuant to 22 U.S.C. 611 *et seq.* The system is also maintained to implement the provisions of 28 CFR 0.72 and 28 CFR Part 5.

PURPOSE OF THE SYSTEM:

The system is maintained to enable the Registration Unit, Counterespionage Section, National Security Division, to implement the various provisions of the Foreign Agents Registration Act of 1938, as amended, 22 U.S.C. 611 *et seq.* The system provides for the public examination of registration statements filed by foreign agents engaged in activities for or on behalf of foreign governments, foreign political parties, or other foreign principals. Public examination helps to insure that the U.S. Government and the people of the United States are informed of the source of information and the identity of persons attempting to influence U.S. public opinion, policy, and laws.

As prescribed by 22 U.S.C. 616(a), (b), and (c), the records in this system that are public records are open to public examination and inspection and copies of the same shall be furnished to every applicant at fees prescribed by 28 CFR 5.601. One copy of every registration statement filed under FARA and one copy of every amendment or supplement thereto filed under FARA shall be forwarded to the Secretary of State for such comment and use as the Secretary of State may determine to be appropriate from the point of view of the foreign relations of the United States.

Public information obtained under FARA, including the names of registrants, copies of

registration statements, or parts thereof, copies of informational materials, or other documents or information filed under FARA, may be furnished to departments and agencies in the executive branch and committees of the Congress.

Other records related to the subject matters described in this system that are not available for public examination may be disclosed as follows.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

To a Member of Congress or staff acting upon the Member's behalf when the Member requests the information on behalf of, and at the request of, the individual who is the subject of the record.

To contractors, grantees, experts, consultants, students, and others performing or working under a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such a violation or charged with enforcing or implementing such law.

To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

A record may be disclosed to designated officers and employees of state, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.

In an appropriate proceeding before a court, or administrative or adjudicative body, where the Department of Justice determines that the records are arguably relevant to the proceeding in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings.

To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

To Federal, state, local, tribal, foreign, or international licensing agencies or associations that require information concerning the suitability or eligibility of an individual for a license or

To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

To a former employee of the Department for purposes of: Responding to an official inquiry from a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee where necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

To such recipients and under such circumstances and procedures as are mandated by statute or treaty.

To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

To appropriate agencies, entities, and persons when (1) The Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or

confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected confirmed compromise and prevent, minimize, or remedy such harm.

To any person or entity that the Registration Unit, Counterespionage Section, National Security Division has reason to believe possesses information regarding a matter within the jurisdiction of the Registration Unit, Counterespionage Section, National Security Division, to the extent deemed to be necessary by the Registration Unit, Counterespionage Section, National Security Division in order to elicit such information or cooperation from the recipient for use in the performance of an authorized activity.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Not applicable

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system are stored on paper, and/or in electronic form. Records are stored in accordance with applicable executive orders, statutes, and agency implementing regulations. Paper records contained in this system are stored manually on index cards and in file jackets. Selected summary data, e.g., name and address of registrant, name of foreign principal, description of activities, and amount of money received, are stored on magnetic disks.

RETRIEVABILITY:

Information and summary data is retrieved by registrant name. Summary data includes: name and address of registrant, name of foreign principal, description of activities, amount of money received, and promotional material disseminated.

SAFEGUARDS:

Some records in this system have been designated as public records by 22 U.S.C. 616.

other records in this system are safeguarded in accordance with applicable laws, rules, policies, including the Department's automated systems security and access policies. Records and technical equipment are maintained in a secured area with restricted access. The use of password protection identification features and other system protection methods restrict access.

RETENTION AND DISPOSAL:

Records are retained and disposed of in accordance with a schedule approved by the National Archives and Records Administration.

SYSTEM MANAGER(S) AND ADDRESS:

Chief, Foreign Agents Registration Unit, Counterespionage Section, National Security Division, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530.

NOTIFICATION PROCEDURE:

Same as the Above.

RECORD ACCESS PROCEDURES:

A request for access to a record from this system shall be made pursuant to the provisions of 28 CFR 5.600 and 5.601.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

RECORD SOURCE CATEGORIES:

The source of information contained in this system is the registrant.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[\[TOP\]](#)

JUSTICE/NSD-003

SYSTEM NAME:

Registration Files of Individuals Who Have Knowledge of, or Have Received Instruction Assignment in, Espionage, Counterespionage, or Sabotage Service or Tactics of a Foreign Government or of a Foreign Political Party.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

U.S. Department of Justice; National Security Division; 950 Pennsylvania Avenue, NW., Washington, DC 20530.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Persons who have registered under 50 U.S.C. 851 *et seq.* as having knowledge of, or have received instruction in, espionage, counterespionage, or sabotage service or tactics of a government or of a foreign political party.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system contains the statement of the registrant and other documents required to be filed under 50 U.S.C. 851. The system is a public record except that certain statements may be withdrawn from public examination pursuant to 50 U.S.C. 853 and 28 CFR 12.40 by the Attorney General having due regard for national security and the public interest.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

This system is established and maintained pursuant to 50 U.S.C. 851 *et seq.* The system

also maintained to implement the provisions codified in 28 CFR part 12.

PURPOSE(S):

The system is maintained to enable the Registration Unit, Counterespionage Section, National Security Division, to implement the various provisions of Title 50, United States Code, Sections 851. The system provides for the public examination of the registration statements filed by certain persons who have knowledge of or have received instruction or assignment in the espionage, counterespionage, or sabotage service or tactics of a foreign government or political party.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

As prescribed by 50 U.S.C. 853, a portion of the records in this system are public records and may be disclosed to any individual, organization, or government agency; non public records, i.e. records withdrawn by the Attorney General from public examinations may be disclosed as follows:

To a Member of Congress or staff acting upon the Member's behalf when the Member requests the information on behalf of, and at the request of, the individual who is the subject of the record.

To contractors, grantees, experts, consultants, students, and others performing or working under a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

To appropriate officials and employees of a federal agency or entity that requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a

security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

A record may be disclosed to designated officers and employees of state, local (including District of Columbia), or tribal law enforcement or detention agencies in connection with hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer, detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.

In an appropriate proceeding before a court, or administrative or adjudicative body, where the Department of Justice determines that the records are arguably relevant to the proceeding in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings.

To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

To Federal, state, local, tribal, foreign, or international licensing agencies or associations that require information concerning the suitability or eligibility of an individual for a license or

To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

To a former employee of the Department for purposes of: responding to an official inquiry from a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee where the Department may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

To such recipients and under such circumstances and procedures as are mandated by

statute or treaty.

To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation case arising from the matters of which they complained and/or of which they were a victim.

To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

To any person or entity that the Registration Unit, Counterespionage Section, National Security Division has reason to believe possesses information regarding a matter within the jurisdiction of the Registration Unit, Counterespionage Section, National Security Division, to the extent deemed to be necessary by the Registration Unit, Counterespionage Section, National Security Division in order to elicit such information or cooperation from the recipient for use in the performance of an authorized activity.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Not applicable.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system are stored on paper, and/or in electronic form. Records are stored in accordance with applicable executive orders, statutes, and agency implementing regulations. Each record contained in this system is stored manually on index cards and in file jackets. An automated alphabetical index is maintained and stored on magnetic disks.

RETRIEVABILITY:

A record is retrieved by name of the individual registrant.

SAFEGUARDS:

Records are safeguarded and protected in accordance with applicable Departmental security procedures.

RETENTION AND DISPOSAL:

Staff is working with NARA to develop an appropriate schedule.

SYSTEMS MANAGER(S) AND ADDRESS:

Chief, Foreign Agents Registration Unit; Counterespionage Section; National Security Division
U.S. Department of Justice; 950 Pennsylvania Avenue, NW., Washington, DC 20530.

NOTIFICATION PROCEDURE:

Same as the above.

RECORD ACCESS PROCEDURE:

A request for access to a record from this system shall be made pursuant to the provisions of 28 CFR 12.40 and 12.41.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

RECORD SOURCE CATEGORIES:

The source of information contained in this system is the registrant.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[\[TOP\]](#)

Office of the Inspector General

JUSTICE/OIG-001

System Name:

Office of the Inspector General Investigative Records.

Security Classification:

The vast majority of the information in the system is Sensitive but Unclassified. However, there is some classified information as well.

System location:

U.S. Department of Justice, Office of the Inspector General (OIG), 950 Pennsylvania Avenue NW., Washington, DC 20530-0001 and 1425 New York Avenue, NW., Suites 7100 and 1310, Washington, DC 20530. During the course of an investigation, records are also kept in the investigations field and area offices, the addresses of which are listed on the OIG's Web site at <http://www.usdoj.gov/oig>.

Categories of individuals covered by the system:

In connection with its investigative duties, the OIG maintains records on the following categories of individuals:

a. Individuals or entities who are or have been the subject of investigations conducted by the OIG, including current and former employees of the Department of Justice; current and former consultants, contractors, and subcontractors with whom the Department has contracted; their employees; grantees to whom the Department has awarded grants and their employees; and such other individuals or entities whose association with the Department relates to the OIG's investigative duties.

violation(s) of the Department's rules of conduct, the Civil Service merit system, and/or criminal or civil law, which may affect the integrity or physical facilities of the Department.

b. Individuals who are or have been witnesses, complainants, or informants in investigations conducted by the OIG.

c. Individuals or entities who have been identified as potential subjects of or parties to a investigation.

Categories of records in the system:

Information relating to investigations including:

a. Letters, memoranda, and other documents describing complaints or alleged criminal, administrative misconduct.

b. Investigative files which include: Reports of investigations and related exhibits, sworn affidavits, and records obtained during the investigation.

Authority for maintenance of the system:

Inspector General Act of 1978, as amended, 5 U.S.C. App. 3.

Purpose(s):

The OIG maintains this system of records in order to carry out its responsibilities pursuant to the Inspector General Act of 1978, as amended. The OIG is statutorily directed to conduct, supervise investigations relating to programs and operations of the Department of Justice, to promote economy, efficiency, and effectiveness in the administration of such programs and operations, and to prevent and detect fraud, waste, and abuse in such programs and operations. Accordingly, the records in this system are used in the course of investigating individuals and entities suspected of having committed illegal or unethical acts and in conducting related criminal prosecutions, civil proceedings, and administrative actions.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records in this system may be disclosed as follows:

- (a) To any criminal, civil, or regulatory law enforcement authority (whether federal, state territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.
- (b) To any individual or entity when necessary to elicit information that will assist an OIG investigation, inspection, or audit.
- (c) To any individual or entity when necessary to elicit information relevant to an OIG decision concerning the hiring, appointment, or retention of an individual; the issuance, renewal, suspension, or revocation of a security clearance; or the letting of a contract.
- (d) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an individual; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance or revocation of a grant or other benefit.
- (e) To appropriate officers and employees of state, local territorial, or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.
- (f) To federal, state, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.
- (g) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
- (h) In an appropriate proceeding before a court, grand jury, or an administrative or adjudicatory body, when the OIG determines that the records are arguably relevant to the proceeding.

an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(i) To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings.

(j) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(k) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(l) To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

(m) To the Office of the Inspector General for the Department of Homeland Security when necessitated by the transfer of Department of Justice functions and employees to the Department of Homeland Security.

(n) To other federal Offices of Inspector General and/or to the President's Council on Integrity and Efficiency for purposes of conducting the external review process required by the Homeland Security Act.

(o) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, who have a need to know such information in order to accomplish an assigned function.

(p) To a former employee of the Department of Justice for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes when the Department requires information and/or consultation assistance from the former employee.

regarding a matter within that person's former area of responsibility.

(q) To appropriate agencies, entities, and persons when (1) the Department suspects or confirmed that the security or confidentiality of information in the system of records has compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (w maintained by the Department or another agency or entity) that rely upon the compromi information; and (3) the disclosure made to such agencies, entities, and persons is reas necessary to assist in connection with the Department's efforts to respond to the susper confirmed compromise and prevent, minimize, or remedy such harm.

(r) To such recipients and under such circumstances and procedures as are mandated federal statute or treaty.

(s) To a governmental entity lawfully engaged in collecting law enforcement, law enforc intelligence, or national security intelligence information for such purposes.

Disclosure to Consumer Reporting Agencies:

Not Applicable.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Information in this system is stored manually in file jackets and electronically in office automation equipment.

Retrievability:

Each OIG investigation is assigned a case number and all records relating to a particular investigation are filed and retrieved by that case number. Records may also be retrieved the surnames of subjects, witnesses, and/or complainants.

Safeguards:

Information is stored in safes, locked filing cabinets, and office automation equipment in secured rooms or in guarded buildings, and is used only by authorized, screened personnel. Manual records are in locked cabinets or in safes and can be accessed by key or combination formula only. Passwords are required to access the automated data.

Retention and disposal:

Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, Job Number NI-60-97-4.

System manager(s) and address:

Office of the General Counsel, Office of the Inspector General, Department of Justice, 900 Pennsylvania Avenue, NW., Room 4726, Washington, DC 20530.

Notification procedure:

Address inquiries to the System Manager listed above.

Record access procedures:

The major part of this system is exempt from this requirement pursuant to 5 U.S.C. 552a(k)(1), and (k)(2). To the extent that this system is not subject to exemption, it is subject to public access. A determination as to exemption shall be made at the time a request for access is received. A request for access to records contained in this system shall be made in writing with the envelope and the letter clearly marked "Privacy Access Request." Include in the request the full name of the individual involved, his or her current address, date and place of birth, notarized signature (or submitted with date and signature under penalty of perjury), and any other identifying number or information which may be of assistance in locating the records. The requester shall also provide a return address for transmitting the information. Access requests shall be directed to the System Manager listed above.

Contesting record procedures:

The major part of this system is exempted from this requirement pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). To the extent that this system of records is not subject to

exemption, it is subject to contest. A determination as to exemption shall be made at the request for contest is received. Requesters shall direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information.

Record source categories:

The subjects of investigations; individuals with whom the subjects of investigations are associated; current and former Department of Justice officers and employees; Federal, local and foreign law enforcement and non-law enforcement agencies; private citizens; witnesses; informants; and public source materials.

Exemptions Claimed for the System:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d); (e)(3), (5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). In addition, the system has been exempted from subsections (c)(3), (d), and (e)(1), pursuant to subsections (k)(1) and (k)(2). Rules have been promulgated in accordance with the requirements of U.S.C. 553(b), (c) and (e), and have been published in the *Federal Register*. See 28 CFR 16.75.

[\[TOP\]](#)

JUSTICE/OIG-004

System name:

Office of the Inspector General Employee Training Records.

System location:

U.S. Department of Justice, Office of the Inspector General, 1425 New York Ave., NW, S
7000, Washington, DC 20530.

Categories of individuals covered by the system:

Employees of the Department of Justice, Office of the Inspector General.

Categories of records in the system:

Information pertaining to formal training requested and attended by OIG employees, including training forms.

Authority for maintenance of the system:

Inspector General Act of 1978, as amended by the Inspector General Amendments of 1992, 5 U.S.C. App. 3.

Purpose(s):

To capture training requests made by OIG employees and to maintain information regarding the training employees have had.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records in this system may be disclosed as follows:

a. Relevant records may be disclosed to an administrative forum, including Ad Hoc forums, which may or may not include an Administrative Law Judge, and which may or may not convene public hearings/proceedings, or to other established adjudicatory or regulatory agencies, e.g., the Merit Systems Protection Board, or other agencies with similar or related statutory responsibilities, where necessary to adjudicate decisions affecting individuals covered by this system, including (but not limited to) decisions to effect any necessary remedial actions, e.g., disciplinary and/or other appropriate personnel actions.

b. A record may be disclosed to the National Archives and to the General Services Administration during a records management inspection conducted under 44 U.S.C. 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating

communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information in this system is stored manually in file jackets and electronically in office automation equipment.

Retrievability:

Information can be retrieved either by surname or social security number.

Safeguards:

Information is stored in filing cabinets and office automation equipment in secured rooms, guarded buildings, and is used only by authorized, screened personnel. Passwords are required to access the automated data.

Retention and disposal:

Records in this system are retained and disposed of in accordance with General Records Schedule 1.

System manager(s) and address:

Office of the General Counsel, Office of the Inspector General, Department of Justice, 900 Pennsylvania Avenue, NW, Room 4261, Washington, DC 20530-0001.

Notification procedure:

Address inquiries to the System Manager listed above.

Record access procedures:

Make requests for access to records from this system in writing to the system manager, clearly mark both the letter and envelope "Privacy Act Request."

Contesting record procedures:

Make all requests to contest or amend information maintained in the system in writing to system manager. State clearly and concisely what information is being contested, the reason for contesting it, and the proposed amendment(s) to the information.

Record source categories:

National Finance Center and employees of the Department of Justice Office of the Inspector General.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/OIG-005

System name:

Office of the Inspector General Firearms Qualification System.

System location:

U.S. Department of Justice, Office of the Inspector General, 1425 New York Ave., NW, S 7100, Washington, DC 20530 and the investigations field offices, the addresses of which are listed on the OIG's website at <http://www.usdoj.gov/oig>.

Categories of individuals covered by the system:

Criminal investigators employed by the Department of Justice, Office of the Inspector General.

Categories of records in the system:

Information relating to the weapons qualifications of OIG criminal investigators, including of qualification and scores.

Authority for maintenance of the system:

Inspector General Act of 1978, as amended by the Inspector General Act of 1988, 5 U.S.C. App. 3, and Attorney General Order 1393–90.

Purpose(s):

To capture information relating to the weapons qualifications of OIG criminal investigators including dates of qualifications and scores.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records in this system may be disclosed as follows:

a. Relevant records may be disclosed to an administrative forum, including Ad Hoc forums which may or may not include an Administrative Law Judge, and which may or may not convene public hearings/proceedings, or to other established adjudicatory or regulatory agencies, e.g., the Merit Systems Protection Board, or other agencies with similar or related statutory responsibilities, where necessary to adjudicate decisions affecting individuals covered by this system, including (but not limited to) decisions to effect any necessary remedial actions, e.g., disciplinary and/or other appropriate personnel actions.

b. A record may be disclosed to the National Archives and to the General Services Administration during a records management inspection conducted under 44 U.S.C. 292906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance.

from the former employee regarding a matter within that person's former area of respon

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Information in this system is stored manually in file jackets and electronically in office automation equipment.

Retrievability:

Information can be retrieved by surname.

Safeguards:

Information is stored in filing cabinets and office automation equipment in secured room guarded buildings, and is used only by authorized, screened personnel. Passwords are required to access the automated data.

Retention and disposal:

Records in this system are retained and disposed of in accordance with General Record Schedule 23.

System manager(s) and address:

Office of the General Counsel, Office of the Inspector General, Department of Justice, 9 Pennsylvania Avenue, NW, Room 4261, Washington, DC 20530-0001.

Notification procedure:

Address inquiries to the System Manager listed above.

Record access procedures:

Make requests for access to records from this system in writing to the system manager,

clearly mark both the letter and envelope "Privacy Act Request."

Contesting record procedures:

Make all requests to contest or amend information maintained in the system in writing to the system manager. State clearly and concisely what information is being contested, the reason for contesting it, and the proposed amendment(s) to the information.

Record source categories:

Employees of the Department of Justice Office of the Inspector General.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

Office of Justice Programs

JUSTICE/OJP-001

System name:

Equipment Inventory.

System location:

Office of Justice Programs, 633 Indiana Avenue NW, Washington, DC 20531.

Categories of individuals covered by the system:

Employees who have filed the following forms in the Office of the Comptroller: Property Sign-out, OJARS Administrative Form 1820/1; Equipment Control Records, OJARS Administrative Form 1820/2.

Categories of records in the system:

Property Sign-out, OJARS Administrative Form 1820/1; Equipment Control Records, OJARS Administrative form 1820/2.

Authority for maintenance of the system:

The system is established and maintained in accordance with 5 U.S.C. 301, 1302.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The property data is used for inventory control.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA): A record from a system of records may be disclosed for a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Information maintained in system is stored on index cards.

Retrievability:

Information is retrieved by name of employee and type of equipment.

Safeguards:

Data is maintained in a locked room.

Retention and disposal:

Documents relating to equipment control are closed when employee leaves agency. Records are destroyed three years thereafter. Operating files are destroyed when an individual retransfers, or is separated from Federal service.

System manager(s) and address:

Comptroller, Office of the Comptroller, Office of Justice Programs, 633 Indiana Avenue NW
Washington, DC 20531.

Notification procedure:

Same as the above.

Record access procedures:

A request for access to a record from the system shall be in writing, with the envelope a letter clearly marked "Privacy Access Request." Access requests will be directed to the Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Individual to whom record pertains, employee's supervisors.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/OJP-002

System name:

Law Enforcement Education System.

System location:

Law Enforcement Assistance Administration, 633 Indiana Avenue NW, Washington, DC

Categories of individuals covered by the system:

Recipients of LEAA Law Enforcement Education Loans and Grants.

Categories of records in the system:

LEEP Master Computer File; LEEP Promissory Note File; LEAA Form 03.

Authority for maintenance of the system:

The system is established and maintained pursuant to 42 U.S.C. 3775

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

To contractors for categories and statistical analysis, educational institutions for record reconciliation, IRS and references listed on application for address verification, reference bankruptcy for claim action, State and local agencies to verify eligibility.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress, Information contained in systems of records maintained by the Department of Justice not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Members or staff requests the information on behalf of and at the requests of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Information maintained in the system is stored on computer magnetic tape and folders.

Retrievability:

Information is retrievable by name of recipient and social security number.

Safeguards:

Computerized information is safeguarded and protected by computer password key and access. Noncomputerized data is safeguard in file room which is locked after business hours. Access is limited to LEAA authorized personnel.

Retention and disposal:

Computerized records are kept indefinitely. Uncollected loans/grants are transferred to soon as determined uncollectable. Cancelled or repaid loan/grants are closed at end of year, held three years, sent to Federal Records Center and destroyed in accordance with instructions from GAO.

System manager(s) and address:

Comptroller, Office of Justice Assistance Research, and Statistics; 633 Indiana Avenue Washington, DC.

Notification procedure:

Same as above.

Record access procedures:

A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." Include in the request the name and personal identifier number. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to System Manager listed above, stating clearly and concisely what information being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information are the recipients of loans/grants and their educational institutions.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/OJP-004

System name:

Grants Management Information System (PROFILE).

System location:

Office of Justice Programs, 633 Indiana Avenue, NW, Washington, DC 20531

Categories of individuals covered by the system:

Included are recipients (grantees) of OJP funds. These include grantees of the National Institute of Justice, the Bureau of Justice Statistics, the Bureau of Justice Assistance, the Office of Juvenile Justice and Delinquency Prevention, the Office of Victims of Crime, and the now defunct Office of Justice Assistance, Research, and Statistics, and the Law Enforcement Assistance Administration. Also included are project monitors and project directors of the grants.

Categories of records in the system:

Grantee and Project Audit File, Financial and Programmatic Compliance Records of the Grantee, Grant Applications, and Grant/Contract Award Computer Data File.

Authority for maintenance of the system:

The system is established and maintained in accordance with U.S.C. 301, 44 U.S.C. 3101, and 31 U.S.C. 3512.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records from this system of records may be disclosed for the purpose of technical review, fiscal or program evaluation to experts in particular subject areas related to the substantial fiscal components of the program.

Release of Information in an Adjudicative Proceeding:

It shall be a routine use of records within this system or any facts derived therefrom, to disseminate them in a proceeding before a court or adjudicative body before which the individual is authorized to appear, when

- i. The OJP, or any subdivision thereof, or
- ii. Any employee of the OJP in his or her official capacity, or
- iii. Any employee of the OJP in his or her individual capacity, where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the OJP determines that the litigation is likely to affect it or its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the OJP to be arguably relevant to the litigation.

Release of Information to the News Media:

Information permitted to be released to the news media and the public pursuant to 28 C.F.R. 50.2 may be made available from systems of records maintained by the Department of Justice, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of Information to Members of Congress:

Information contained in systems of records maintained by the Department of Justice not otherwise required to be released pursuant to 5 U.S.C. 522, may be disclosed as a routine use of records to a member of Congress or staff acting upon the member's behalf when the member or staff requests the information on behalf of and at the request of the individuals who are the subjects of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA). A record from a system of records may be disclosed for a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored on computer disc for use in a computer environment.

Retrievability:

Data is retrievable by name of individual covered by the system.

Safeguards:

Information in the system is safeguarded and protected by computer password key. Direct access is limited to computer personnel.

Retention and disposal:

Data is maintained for current fiscal year and previous fiscal years in master file. Data is destroyed, but maintained for historical purposes.

System manager(s) and address:

Comptroller, Office of Justice Programs, 633 Indiana Avenue, NW, Washington, DC 205

Notification procedure:

Same as above.

Record access procedures:

A request for access to a record from this system shall be made in writing with the envelope and letter clearly marked "Privacy Access Request." Include in the request the name and grant/contract number. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their requests to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in the system are grantees, applicants for award, and project monitors.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/OJP-005

System name:

Financial Management System.

System location:

Office of Justice Program (OJP), 633 Indiana Avenue, NW, Washington, DC 20531.

Categories of individuals covered by the system:

Recipients of OJP, OJARS, LEAA, NIL, BIS, and OJJDP funds; Employees.

This system contains information concerning (a) current and past recipients of OJP funds including those from the National Institute of Justice, the Bureau of Justice Assistance, Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, Office for Victims of Crime, and the now defunct Office of Justice Assistance, Research Statistics, and Law Enforcement Assistance Administration; (b) OJP employees; and (c) individuals on whom vouchers are submitted requesting payment for goods or services rendered (except payroll vouchers for Department of Justice employees), including vendors, contractors, travelers, and employees.

Categories of records in the system:

Employee Travel Files; Time and Attendance Files; Government Travel System and Government Charge Cards; Government Transportation Request; Paid Vendor Document File, all vouchers processed, i.e., all documents required to reserve, obligate, process an effect collection or payment of funds. (Excluded from the system are payroll vouchers.)

Authority for maintenance of the system:

5 U.S.C. 301, 31 U.S.C. 3512, and 44 U.S.C. 3101.

Purpose(s):

After processing the vouchers, OJP and the Justice Management Division use the records to maintain individual financial accountability; to furnish statistical data (not identified by personal identifiers); to meet both internal and external audit and reporting requirements; and to provide information to Administrative Officers from the Offices, Boards, and Divisions and the OJP with information on vouchers by name and social security number for agency financial management.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Release of information in an adjudicative proceeding:

It shall be a routine use of records within this system or any facts derived therefrom, to disseminate them in a proceeding before a court or adjudicative body before which the individual is authorized to appear, when

- i. The OJP, or any subdivision thereof, or
- ii. Any employee of the OJP in his or her official capacity, or
- iii. Any employee of the OJP in his or her individual capacity, where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the OJP determines that the litigation is likely to affect it or its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the OJP to be arguably relevant to the litigation.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Service Administration (GSA). A record from a system of records may be disclosed as a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes

responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Computerized discs, filed folders.

Retrievability:

Name, social security numbers, digital identifiers assigned by accounting office.

Safeguards:

Information contained in the system is unclassified and maintained in accordance with OMB procedures. Manual information in the system is safeguarded in locked file cabinets. Operational access to information maintained on computer discs is controlled by passwords. These keys are issued only to employees who have a need to know to perform job functions relating to financial management and accountability. Access to manual files is also limited to employees who have a need for the records in the performance of their official duties.

Retention and disposal:

Employee travel files, time and attendance files and Government transportation files are retained at end of fiscal year, held three years thereafter.

Payment documents are retained for three fiscal years (current and two years). The payment documents and the aforementioned files are then shipped to a General Services Administration's Federal Records Center for storage and subsequent destruction in accordance with instructions of the General Accounting Office. Computerized discs are retained indefinitely.

System manager(s) and address:

Comptroller, Officer of Justice Programs, 633 Indiana Avenue, NW., Washington, DC 20

Notification procedure:

Same as above.

Record access procedures:

A request for access to a record from this system shall be made in writing with the envelope and letter clearly marked "Privacy Access Request." Access requests will be directed to System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in the system are the individuals to whom the information pertains.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/OJP-006

System name:

Congressional and Public Affairs System.

System location:

Office of Justice Programs (OJP), 633 Indiana Avenue, NW, Washington, DC 20531.

Categories of individuals covered by the system:

Members of Congress, and other public figures.

Categories of records in the system:

Correspondence with Congressional Committees, members of Congress, and the general public. The file also contains biographical data, speeches, press releases, and photographic files relating to public figures.

Authority for maintenance of the system:

The system is established and maintained in accordance with 5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information in this system is used or may be used in response to inquiries from the general public or member of Congress.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and

General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information is indexed on a correspondence control log and stored in file folders.

Retrievability:

Information is retrieved by name of the member of Congress who is the correspondent, the name of the public figure.

Safeguards:

Records are maintained in file cabinets. Entrance to the building is controlled by requiring employee identification or security clearance procedures. Records are used by employees on a need to know basis only.

Retention and disposal:

Records are retained for two years, then retired to Federal Records Center. Six years thereafter, records are destroyed.

System manager(s) and address:

Director, Office of Congressional and Public Affairs, Office of Justice Programs, 633 Indiana

Avenue NW, Washington, DC 20531.

Notification procedure:

Same as the above.

Record access procedures:

A request for access to a record from the system shall be in writing, with the envelope a letter clearly marked "Privacy Access Request." Access requests will be directed to the Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information are Congressional members.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/OJP-007

System name:

Public Information System.

System location:

Office of Justice Assistance, Research and Statistics, 633 Indiana Avenue NW, Washington, DC 20531.

DC 20531.

Categories of individuals covered by the system:

Public figures.

Categories of records in the system:

Biographical, Morgue, and Speech files, Photograph files.

Authority for maintenance of the system:

The system is maintained and established in accordance with 5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Available to the public under the Freedom of Information Act.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specified information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 5 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose

relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in system is stored in file folders.

Retrievability:

Information is retrieved by name of person to whom information pertains.

Safeguards:

This information is of a nonconfidential nature and maintained pursuant to LEAA Handbook Instruction HB 1330.2.

Retention and disposal:

Records are retained for four years, retired to Federal Records Center, and destroyed pursuant to Disposal Instructions in LEAA Handbook Instruction HB 1330.2.

System manager(s) and address:

Director, Office of Public Information, Office of Justice Assistance, Research and Statistics
Indiana Avenue NW, Washington, DC 20531.

Notification procedure:

Same as the above.

Record access procedures:

A request for access to a record from the system shall be in writing, with the envelope a letter clearly marked "Privacy Access Request." Access requests will be directed to the Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Newspaper, magazine and press service teletype clippings as well as individual to whom information pertains.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/OJP-008

System name:

Civil Rights Investigative System.

System location:

Office of Justice Programs (OJP).

Categories of individuals covered by the system:

Individuals affected by any OJP project for which the agency has compliance responsibility.

including grantees, subgrantees, contractors, subcontractors, employees, and applicants who have made complaints of discrimination. OJP includes the National Institute of Justice, the Bureau of Justice Statistics, the Bureau of Justice Assistance, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Also included are individuals who are the subjects of civil rights compliance records of the now defunct Office of Justice Assistance, Research, and Statistics, and the Law Enforcement Assistance Administration.

Categories of records in the system:

Civil Rights Complaint Control Files: Civil Rights Litigation Reference Files.

Authority for maintenance of the system:

42 U.S.C. 3789d, 42 U.S.C. 10604(e), 29 U.S.C. 794, 42 U.S.C. 2000d, 20 U.S.C. 1681, U.S.C. 5601, and 42 U.S.C. 1601.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

OJP uses information in this system to investigate complaints and to obtain compliance with civil rights laws. Other such users of the information are appropriate State agencies, Civil Rights Division of the Justice Department, State Governors and Attorneys General, Office of Federal Contract Compliance, Equal Employment Opportunity Commission, Office of Federal Revenue Sharing, and the United States Commission on Civil Rights, Department of Health and Human Services, Department of Education and OJP. OJP may also use this information for agency project evaluation, technical assistance, and training.

Release of information in an adjudicative proceeding:

It shall be a routine use of records within this system or any facts derived therefrom, to disseminate them in a proceeding before a court or adjudicative body before which the individual is authorized to appear, when

- i. The OJP, or any subdivision thereof, or
- ii. Any employee of the OJP in his or her official capacity, or

- iii. Any employee of the OJP in his or her individual capacity, where the Department of Justice has agreed to represent the employee, or
- iv. The United States, where the OJP determines that the litigation is likely to affect it or its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the OJP to be arguably relevant to the litigation.

Release of information to the news media:

Information permitted to be released to the news media and the public pursuant to 28 C.F.R. 50.2 may be made available from systems of records maintained by the Department of Justice, unless it is determined that release of the specific information in the context of a particular request would constitute an unwarranted invasion of personal privacy.

Release of information to members of congress:

Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA):

A record from a system of records may be disclosed as a routine use to NARA and GSA for records management inspections conducted under the authority of 44 U.S.C. 2904 and

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Information in the system is stored in file folders and on index cards.

Retrievability:

Information is retrieved by name of the individual or organization against whom the complaint was made.

Complaint case files are not retrievable by information identifiable to the individual complainant.

Safeguards:

Information is kept in locked file cabinets and combination safe. Access is limited to investigative personnel.

Retention and disposal:

All investigative information is destroyed ten years after the investigation is completed.

System manager(s) and address:

Office of Civil Rights Compliance, Office of Justice Programs, 633 Indiana Avenue NW, Washington, DC 20531.

Notification procedure:

Same as the above.

Record access procedures:

A request for access to a record containing civil rights investigatory material shall be made in writing with the envelope and letter clearly marked "Privacy Access Request" to the Civil Rights Compliance Officer.

System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

The information contained in this system was received from individual complainants, witness grant files, respondents, official State and Federal records.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsection (d) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c), and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/OJP-009

System name:

Federal Advisory Committee Membership Files.

System location:

Office of Justice Programs (OJP), 633 Indiana Avenue NW, Washington, DC, 20531.

Categories of individuals covered by the system:

Individuals who have been or are presently members of or are being considered for membership on advisory committees within the jurisdiction of the OJP.

OJP includes the former Office of Justice Assistance, Research, and Statistics, the former

Enforcement Assistance Administration, National Institute of Justice, Bureau of Justice Assistance, Office of Juvenile Justice and Delinquency Prevention, and the Office of Vic Crime.

Categories of records in the system:

Correspondence, documents relating to committee members, biographical data, and Committee membership forms.

Authority for maintenance of the system:

Federal Advisory Committee Act, 5 U.S.C. App. I et seq.; 5 U.S.C. 301; 44 U.S.C. 3101.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Annual Report to the President; administrative reports to OMB and other federal agencies

Release of information to the news media:

Information permitted to be released to the news media and the public pursuant to 28 C 50.2 may be made available from systems of records maintained by the Department of Justice, unless it is determined that release of the specific information in the context of a particular request would constitute an unwarranted invasion of personal privacy.

Release of Information to the National Archives and Records Administration (NARA) and General Services Administration (GSA).

A record from a system of records may be disclosed as a routine use to NARA and GSA records management inspections conducted under the authority of 44 U.S.C. 2904 and

Release of Information to Congress.

Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject

the record.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information in system is stored in file folders.

Retrievability:

Information is retrieved by name of individual.

Safeguards:

Data is maintained in file cabinets. The entrance to the building requires building pass card and security sign-in.

Retention and disposal:

The data is placed in an inactive file upon discontinuance of membership, held for two years and then retired to the Federal Records Center.

System manager(s) and address:

Federal Advisory Committee Officer, Office of General Counsel, Office of Justice Programs
633 Indiana Avenue, NW, Washington, DC 20531.

Notification procedure:

Same as the above.

Record access procedures:

A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." Access requests will be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information are supplied directly by individuals about whom the record pertains, references, recommendations, program personnel, and biographical reference books.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/OJP-010

System name:

Technical Assistance Resource Files.

System location:

Office of Juvenile Justice and Delinquency Prevention, 633 Indiana Avenue NW, Washington, DC 20531.

Categories of individuals covered by the system:

Consultants with expertise in criminal justice systems.

Categories of records in the system:

The system consists of resumes and other documents related to technical assistance re

Authority for maintenance of the system:

The system is maintained under authority of 44 U.S.C. 3101 and 42 U.S.C. 5614(b)(6).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The system is used to determine the qualifications and availability of individuals for tech assistance assignments. Users are State Criminal Justice Councils, and the Office of Ju Justice and Delinquency Prevention.

Release of information to the new medias:

Information permitted to be released to the news media and the public pursuant to 28 C 50.2 may be made available from systems of records maintained by the Department of , unless it is determined that release of the specific information in the context of a particu would constitute an unwarranted invasion of personal privacy.

Release of information to members of Congress:

Information contained in systems of records maintained by the Department of Justice, n otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or sta requests the information on behalf of and at the request of the individual who is the sub the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration:

A record from a system of records may be disclosed as a routine use to NARA and GSA records management inspections conducted under the authority of 44 U.S.C. 2904 and

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of respon

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Information contained in the system is on hard copy and stored in file cabinets.

Retrievability:

Information is manually retrieved by the name of the individual.

Safeguards:

Records are stored in file cabinets. Admittance to the building in which they are stored requires a building pass or an individual signature at the main entrance to the building.

Retention and disposal:

Records are placed in an inactive file at the end of the fiscal year in which final use was completed. They are held two years in the inactive file; then transferred to the Federal Records Center. Records are destroyed after six years.

System manager(s) and address:

Technical Assistance Coordinator; Division Director of Program area in which records are sought in the Office of Juvenile Justice and Delinquency Prevention, Office of Justice

Programs, 633 Indiana Avenue NW, Washington, DC 20531.

Notification procedure:

Address inquiries to the system manager(s) at the above address.

Record access procedures:

A request for access to a record contained in this system shall be made in writing with the envelope and letter clearly marked "PRIVACY ACCESS REQUEST." Include in the request the name and grant/contract number for the record desired. Access requests will be directed to the system manager(s) listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their requests to the system manager(s) listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in this system are those individuals to whom the information pertains.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/OJP-011

System name:

Register Users File—National Criminal Justice Reference Service (NCJRS).

System location:

National Criminal Justice Reference Service, 1600 Research Blvd., Rockville, MD 20850

Categories of individuals covered by the system:

The system contains information on those individuals engaged in criminal justice activities, citizen groups and academicians.

Categories of records in the system:

The system provides a record of registrants who request reference services and products from NCJRS.

Authority for maintenance of the system:

The system is maintained and established in accordance with 42 U.S.C. 3721.

Purpose(s):

Information in this system is used as a mailing list to supply registrants requesting services from NCJRS with information or products.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information permitted to be released to the news media and the public pursuant to 29 C.F.R. 50.2 may be made available unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Information, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is subject of the record.

A record may be disclosed as a routine use to the National Archives and Records Administration and the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information is stored on magnetic disc pack for use in a computer environment.

Retrievability:

Information is retrieved by the name and user identity number of the individual or organization requesting information.

Safeguards:

Information is maintained in the NCJRS Data Services Center which is a secured area. Security identity cards are required for admittance to the area.

Retention and disposal:

Information is retained until the individual no longer wishes to utilize the service. Upon notification by an individual that he no longer wishes to use the service, or by lack of response of user to Annual Renewals, his record is electronically purged from the film.

System manager(s) and address:

User Services Coordinator, National Criminal Justice Reference Service, PO Box 6000, Rockville, MD 20850.

Notification procedure:

Address inquires to the system manager(s) at the above address.

Record access procedure:

A request for access to a record contained in this system shall be made in writing with the envelope and letter clearly marked: 'PRIVACY ACCESS REQUEST.' Access requests will be directed to the system manager(s) at the above address.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their requests to the system manager(s) listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources for the information contained in this system are those individuals covered by this system.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/OJP-012

System name:

Public Safety Officers Benefits System.

System location:

Bureau of Justice Assistance, Office of Justice Programs, (OJP), 810 Seventh Street, N.W., Washington, DC 20531.

Categories of individuals covered by the system:

Public Safety Officers who are permanently and totally disabled by a traumatic injury in of duty and the surviving beneficiaries of public safety officers who died while in the line duty.

Categories of records in the system:

This system contains an index by claimant survivor and deceased or permanently and c Public Safety Officers; case files of eligibility documentation; and benefit payment recor

Authority for maintenance of the system:

Authority for maintaining this system exists under 42 U.S.C. 3796 and 44 U.S.C. 3103.

Purpose(s):

Information contained in this system is used or may be used to determine and record el of Public Safety Officers under the Public Safety Officers Benefits Act and the Federal l Enforcement Dependents Assistance Act.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records, or any information derived therefrom, may be disclosed as follows: To State ar agencies to verify and certify eligibility for benefits; to researchers for the purpose of researching the cause and prevention of public safety officer line of duty deaths; to app Federal agencies to coordinate benefits paid under similar programs; in a proceeding b court or adjudicative body before which the OJP is authorized the appear, when i. The (any subdivision thereof, or ii. Any employee of the OJP in his or her official capacity, or employee of the OJP in his or her individual capacity, where the Department of Justice l agreed to represent the employee, or iv. The United States, where the OJP determines litigation is likely to affect it or any of its subdivisions, is a party to litigation or has an int litigation and such records are determined by the OJP to be arguably relevant to the liti to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined tha release of the specific information in the context of a particular case would constitute an

unwarranted invasion of personal privacy; to the National Archives and Records Administration (NARA) and to the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906; to a Member of Congress or acting upon the Member's behalf when the Member or staff requests the information on of and at the request of the individual who is the subject of the record.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Information in this system is maintained on a master index, in folders and in an automated information system.

Retrievability:

Information is retrieved by name of claimant, name of deceased or disabled Public Safety Officer, and case file number.

Safeguards:

Computerized information is safeguarded and protected by computer password key and access. Noncomputerized data is safeguarded in locked cabinets. All files are maintained in a secure building.

Retention and disposal:

Files are retained in the Public Safety Officer Benefits (PSOB) Office on hard copy and computer network. Files will be disposed of pursuant to OJP Handbook 1330.2A.

System manager(s) and address:

PSOB Program Officer, Bureau of Justice Assistance, Office of Justice Programs, 810 S Street, NW, Washington, DC 20531.

Notification procedure:

Same as above.

Record access procedures:

Request for access to a record from this system should be made in writing with the envelope and the letter clearly marked "Privacy Access Request." Access requests will be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above and state clearly and concisely what information is being contested, the reason for contesting it and the proposed amendment to the information sought.

Record source categories:

Public agencies including employing agency, beneficiaries, educational institutions, physicians, hospitals, official state and Federal Documents.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/OJP-13

System name:

Denial of Federal Benefits Clearinghouse System (DEBAR).

System location:

Office of Justice Programs; Denial of Federal Benefits Program (DFBP), 810 Seventh St NW, Washington, DC 20531.

Categories of individuals covered by the system:

Any individual convicted of a Federal or State offense involving drug trafficking or possession of a controlled substance who has been denied Federal benefits by Federal or State court; any individual convicted of defense-contract related felonies.

Categories of records in the system:

Records include any which are necessary to identify a person who is convicted of drug trafficking or possession of a controlled substance and sentenced by a State or Federal court to a denial of Federal benefits pursuant to 21 U.S.C. 862; convicted of a defense contract related felony and sentenced by a Federal judge to a denial of Federal benefits pursuant to 21 U.S.C. 2408; and any records which may be relevant to consideration of employment or Federal benefits. For example, included are current and prior offense and arrest data such as type of offense for which the individual is being placed on a list of ineligibles to receive Federal benefits; court and sentencing data, including community service sentencing, if any; identification of benefits to be denied and status thereof, including period of denial; and treatment data. Records also include court orders, notices from U.S. Attorneys concerning convictions, Federal agency benefit listings, and a log of groups or individuals requesting information about an offender's denials.

Authority for maintenance of the system:

The system is established and maintained in accordance with 21 U.S.C. 862 and 10 U.S.C. 2408(c).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records, or any information derived therefrom, may be disclosed as follows: to the Gen

Services Administration (GSA) for inclusion in the publication, "Lists of Parties Excluded Federal Procurement and Nonprocurement Programs," more commonly known as the "Debarment List;" to Federal agencies, certain private entities, certain defense-related contractors and first-tier subcontractors that require access to such records in order to v disqualifying convictions prior to awarding a Federal benefit, as defined under 21 U.S.C or employment under 10 U.S.C. 2408(a); to the sentencing court for verification purpose proceeding before a court or adjudicative body before which the OJP is authorized to ap when: i. The OJP, or any subdivision thereof; or ii. Any employee of the OJP in his or he official capacity; or iii. Any employee of the OJP in his or her individual capacity, where t Department of Justice has agreed to represent the employee; or iv. The United States, v the OJP determines that the litigation is likely to affect it or any of its subdivisions, is a p litigation or has an interest in litigation and such records are determined by the OJP to l arguably relevant to the litigation; to the news media and the public pursuant to 28 CFF may be made available from systems of records maintained by the Department of Justic unless it is determined that release of the specific information in a particular case would constitute an unwarranted invasion of personal privacy; to a Member of Congress or a s person acting on the Member's behalf, when the Member or staff officially requests the information on behalf of, and at the request of, the individual who is the subject of the r to the National Archives and Records Administration (NARA) and the General Services Administration (GSA) in records management inspections conducted under the authorit U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or profess licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related o official purposes where the Department requires information and/or consultation assista from the former employee regarding a matter within that person's former area of respon

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Information maintained in the system is stored in a database on a secured computer ne as well as in manual file folders.

Retrievability:

Data is retrievable by name of individual, social security number, and case number.

Safeguards:

Information contained in the system is maintained in accordance with DFBP procedures Manual information in the system is safeguarded in locked file cabinets within a limited room in a limited access building. Access to manual files is limited to personnel who have need for files to perform official duties. Operational access to information maintained on dedicated computer system, is controlled by levels of security provided by password keys to prevent unauthorized entry, and an audit trail of accessed information. Access is also limited to personnel who have a need to know to perform official duties.

Retention and disposal:

Data is maintained for current and prior years in a master file. Data is not destroyed, but maintained for historical purposes.

System manager(s) and address:

Director, DFBP, Office of Justice Programs, 810 Seventh Street, NW, Washington, DC 20032

Notification procedure:

Same as above.

Record access procedures:

A request for access to a record from the system shall be in writing, with the envelope a letter marked "Privacy Access Request." Direct the access request to the System Manager listed above. Identification of individuals requesting access to their records will include fingerprinting (28 CFR 20.34).

Contesting records procedures:

An individual desiring to contest or amend information maintained in the system should

the request to the System Manager listed above. The request should state clearly and concisely the information being contested, the reasons for contesting the information, and proposed information amendment(s) sought.

Record source categories:

Sources of information contained in the system are Federal and State courts, individuals convicted of certain drug offenses, individuals convicted of defense-contract related felonies, United States Attorneys, and Federal agencies.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/OJP—014

System Name:

Victims of International Terrorism Expense Reimbursement Program.

Security Classification:

Unclassified.

System Location:

Original records will be kept at the Office of Justice Programs (OJP), 810 Seventh Street, Washington, DC 20531. Copies of records may be kept at locations of authorized contractors. The Office for Victims of Crimes (OVC) will have access to any/all data base(s) established by an OVC contractor and the data base(s) will be maintained internally or placed on the OJP/OVC server.

Categories of Individuals Covered by the System:

Claimants seeking expense reimbursement under the program, individuals filing claims

behalf of claimants, and individuals referenced in claims or related documents.

Categories of Records in the System:

Records in the system include: Claim forms filed by or on behalf of claimants seeking reimbursement under the program; records from telephone contacts or inquiries; documents submitted in support of the claims; medical, personal, employment, financial, and other records obtained or generated to process claims.

Authority for Maintenance of the System:

Authority for maintaining this system exists under the Victims of Crime Act ("VOCA"), 42 U.S.C. 10601 et seq.; 10604 (Administrative provisions).

Purpose of Records Maintained in the System:

Information contained in this system may be used to determine and record eligibility of claimants under the Victims of Crime Act, as amended, and any reimbursement provided under the Act, and to track claim status. For individuals who are eligible, see 42 U.S.C. 10603c. The term "victim" means "a person who—(i) suffered direct physical or emotional injury or death as a result of international terrorism occurring on or after December 21, 1988 with respect to which an investigation or prosecution was ongoing after April 24, 1996; and (ii) on the date on which the international terrorism occurred, was a national of the United States or an officer or employee of the United States Government." [42 U.S.C. 10603c(3)(A) (i) and (ii)]

Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses:

Records, or any information derived therefrom, may be disclosed as follows:

- A. To appropriate Federal, State and local agencies to coordinate expense reimbursement paid under similar programs;
- B. To Federal, State and local agencies to verify and certify eligibility for expense reimbursements;
- C. In an appropriate proceeding before a court, or administrative or adjudicative body, with respect to a claim for reimbursement.

the Department of Justice determines that the records are arguably relevant to the proceeding or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

D. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

E. To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

F. Limited information may be disclosed to relief organizations/agencies, as appropriate, in the event of international terrorism.

G. To foreign compensation programs and/or foreign governments to coordinate payment of expense reimbursements and/or to ensure no duplication of payments.

H. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

I. Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, foreign, or tribal, law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.

J. To appropriate officials and employees of a Federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit.

K. To the White House (the President, Vice President, their staffs, and other entities of the Executive Office of the President (EOP)) for Executive Branch coordination of activities v

relate to or have an effect upon the carrying out of the constitutional, statutory, or other or ceremonial duties of the President or Vice-President.

L. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

M. To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

N. The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee, if necessary, for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing Records in the System:

Storage:

Information in this system is maintained on a master index, in folders, and in an automated system.

Retrievability:

Data is retrieved by name and address of claimant, name and address of deceased or injured victim, by terrorism incident, by type of service provider/service rendered to victim, by nationality (Foreign Service National (FSN) vs. U.S. National), by social security number, date of birth, and individual case file number.

Safeguards:

Computerized information is safeguarded and protected by computer password key and access. Electronic record retention is also protected by "firewalls." Operational access to

information maintained on a dedicated computer system, is controlled by levels of security provided by password keys to prevent unauthorized entry, and audit trail of accessed information. Access to manual files is limited to personnel who have a need for files to perform official duties and is safeguarded in locked file cabinets. All files are maintained in a secure building.

Retention and Disposal:

Files are retained on hard copy and on a computer database. All claim files and automated data pertaining to a claim are destroyed 10 years after the date the claim has been fully processed and/or payment made, as approved by the National Archives and Records Administration (NARA). Automated data is retained in its most current form only, however, as information is updated, outdated information is deleted. The schedule was approved and signed by the NARA Archivist on September 30, 2004.

System Manager(S) and Address:

Terrorism and International Victim Assistance Services Division, Office for Victims of Crime
Office of Justice Programs, 810 7th Street, NW., Washington, DC 20531.

Notification Procedure:

Inquiries concerning this system should be addressed to the system manager listed above or FOI/PA Personnel.

Record Access Procedures:

Request for access to a record from this system shall be made in writing with the envelope or letter clearly marked "Freedom of Information/Privacy Act Request." The request shall include a general description of the records sought and must include the requester's full current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

Contesting Record Procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, state clearly and concisely what information

is being contested, the reason for contesting it, and the proposed amendment to the information sought.

Record Source Categories:

Public agencies including investigating agency, employing agency, claimants, education institutions, physicians, hospitals, official State and Federal documents.

Exemptions Claimed For The System:

None.

[\[TOP\]](#)

Office of Legal Counsel

JUSTICE/OLC-001

System name:

Attorney Assignment Reports.

System location:

Office of Legal Counsel, U.S. Department of Justice, 10th and Constitution Avenue, NW Washington, DC.

Categories of individuals covered by the system:

Attorneys employed in the Office of Legal Counsel, U.S. Department of Justice at the time each report was filed.

Categories of records in the system:

The system consists of memoranda addressed to the Assistant Attorney General by each attorney at periodic intervals listing current assignments. Some reports also list completed assignments, projected workload and anticipated leave.

Authority for maintenance of the system:

These records are kept for administrative convenience pursuant to 5 U.S.C. 301 and 44 3101.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information from the system is not used outside the Department except to advise Executive Branch agencies as to the identity of the attorney working on a specific assignment, when inquiry is made.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 5 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

The Assistant Attorney General, each of his Deputies, the Administrative Officer and the attorney who filed the report each have copies. Some are retained chronologically in file folders, some alphabetically in note books.

Retrievability:

Information may be retrieved by name, alphabetically, or chronologically.

Safeguards:

Information is maintained in offices occupied during the day and locked at night.

Retention and disposal:

The Assistant Attorney General's file is chronological and is maintained for three months. Attorneys may retain their copies indefinitely, others are kept for about two years and disposed of.

System manager(s) and address:

Assistant Attorney General, Office of Legal Counsel, U.S. Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Address inquiries to the System Manager, the Administrative Officer or the two Deputies above address.

Record access procedures:

A request for access to a record from this system may be made in person or in writing, specifying the name of the attorney and the dates of reports requested.

Contesting record procedures:

Any requests for correction should be addressed to the System Manager.

Record source categories:

Information is supplied by the attorneys employed by the Office of Legal Counsel on the report is filed.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/OLC-002

System name:

Office of Legal Counsel Central File.

System location:

U.S. Department of Justice, Office of Legal Counsel, 10th and Constitution Avenue, NW
Washington, DC 20530.

Categories of individuals covered by the system:

The system will permit retrieval of information concerning persons mentioned in the legal opinions, memoranda, correspondence, testimony and other writings of the Office of Legal Counsel. These will include:

(A) Addresses, authors and employees of the Office of Legal Counsel whose name appears in memoranda, opinions, correspondence, testimony and other writings of the Office;

(B) Individuals who are the subject of opinions, particularly on such subjects as conflict of interest, employee standards of conduct, and immigration;

- (C) Attendees at meetings described in a memorandum included in the file;
- (D) Litigants and judges identified in connection with reported court decisions and pending cases described in memoranda; and
- (E) Other individuals identified in connection with questions presented to the Office of Legal Counsel for resolution or comment.

Categories of records in the system:

The system consists of memoranda, correspondence, testimony and other writings of the Office of Legal Counsel from 1945 to the present.

Authority for maintenance of the system:

The system is maintained pursuant to the responsibilities of the Office of Legal Counsel set forth in 28 CFR 0.25.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information contained in this system is provided to the following categories of users for the purposes stated:

- (A) Access to the computerized files of the Office of Legal Counsel will be confined to employees of the Office of Legal Counsel and other employees of the Department of Justice with specific permission.
- (B) With the approval of the agency that requested the opinion, selected recent opinions of the Office of Legal Counsel will be published for general use, but personal information about individuals will be deleted if release of that information would constitute a clearly unwarranted invasion of personal privacy;
- (C) Unpublished opinions of the Office of Legal Counsel are ordinarily made available upon request to third parties consistent with the Freedom of Information Act.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

The indices are maintained on 5 x 7 cards in a master subject-matter index on all Office of Legal Counsel memoranda, opinions, correspondence, testimony and other writings. In addition, to facilitate Freedom of Information Act/Privacy Act searches, an alphabetical assortment of cards has been established within the immigration and conflict of interest indices which contain the names of individuals who are the subjects of these opinions. These are, in effect, cross-indices to a small portion of the Office of Legal Counsel's overall operations that are otherwise indexed and retrieved according to subject matter. These indices are maintained to assist in the retrieval of opinions and memoranda from chronological files. However, because the system is undergoing gradual conversion to a computerized system to facilitate legal research, some opinions are also now stored on magnetic disks. Even though the software design creates the capability for name retrieval, the purpose of the design is to facilitate retrieval by legal subject matter and the Office of Legal Counsel will continue to use the system in this manner.

Retrievability:

The alphabetical card index on conflict of interest and immigration opinions will be retrieved by name. In addition, while that information which has been entered into the computer to date may be retrieved by name, all information, except that on conflict of interest and immigration opinions, will ordinarily continue to be retrieved by legal subject matter since the Office has a need to focus on a name in legal research.

Safeguards:

Index cards and chronological files are kept in locked offices when unattended. Access restricted to those personnel with a need to know.

The compilation of Office of Legal Counsel opinions available on magnetic tape is subject to two access limitations designed to insure that only authorized personnel of the Office of Legal Counsel have access. First, the opinions in the computer system can be retrieved only by those persons having a specified identification number, and numbers are assigned only to personnel of the Office of Legal Counsel. Second, there is an access code word in addition to the identification number required for access to the opinions, and the code word is made known only to the Office of Legal Counsel personnel.

During the period in which new opinions are being computerized an exception to these restrictions is made so that the contracting assistant in the Justice Management Division overseeing the computerization also has access to the opinions.

Retention and disposal:

The records will be maintained indefinitely.

System manager(s) and address:

Administrative Officer, Office of Legal Counsel, U.S. Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Inquiries should be addressed to the Assistant Attorney General, Office of Legal Counsel at the address above.

Record access procedures:

Same as above.

Contesting record procedures:

Same as above.

Record source categories:

General legal research sources and individuals and agencies requesting opinions from Office of Legal Counsel.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

Office of Legal Policy

JUSTICE/OLP-002

System name:

United States Judges Records System.

System location:

Office of the Legal Policy, United States Department of Justice, 10th and Constitution A NW, Washington, DC 20530.

Categories of individuals covered by the system:

The system encompasses every United States Judge except those appointed to the United States Court of Military Appeals and Tax Court.

Categories of records in the system:

This system of records consists of records folders which may contain up to five sections. The personnel section contains general, personnel-type information and includes such items as biographical sketches, oaths of office, copies of commissions, nomination letter, qualification statements, letters of recommendation, and copies of notifications of appointment. The character section contains completed or portions of on-going background investigations matters related thereto. The Congressional section contains Congressional and other personnel

type recommendations regarding appointment. The complaint section contains correspondence from individuals or groups complaining about office holders. The protest section contains correspondence, if any exists, protesting the appointment of candidate

Authority for maintenance of the system:

These records are maintained pursuant to 5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Generally, these records are used only for internal Department of Justice purposes. Prior to appointment, routine uses would include those specified for the Presidential Appointee Candidate Record System.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 5 U.S.C. 2904 and 2906.

Release of information to the Judicial Branch of the Federal Government: Information may be disclosed to members of the Judicial Branch of the Federal Government in response to a specific request where disclosure appears relevant to the authorized function of the receiving judicial office of the court.

Release of information to civil or criminal law enforcement agencies: Information may be disclosed to any civil or criminal law enforcement agency, whether Federal, State, local, foreign, which requires information relevant to a civil or criminal investigation.

Release of information to agencies regarding the hiring or retention of employees: Information may be disclosed to officials and employees of the White House or any Federal agency requires information relevant to an agency decision concerning the hiring, appointment, retention of an employee; the issuance of a security clearance; the execution of a security suitability investigation; the classification of a job; or the issuance of a grant or benefit.

Release of information to Federal, State, and local licensing agencies: Information may be disclosed to Federal, State, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

Release of information before a court or adjudicative body: Information may be disclosed in a proceeding before a court or adjudicative body before which the Office of Legal Policy is authorized to appear when (a) the Office of Legal Policy, or any subdivision thereof, or any employee of the Office of Legal Policy in his or her official capacity where the Department of Justice has agreed to represent the employee, or (d) the United States, where the Office of Legal Policy determines that the litigation is likely to affect it or any of its subdivisions, is involved in litigation or has an interest in litigation and such records are determined by the Office of Legal Policy to be arguably relevant to the litigation.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

These records are maintained in paper folders.

Retrievability:

Information is retrieved by use of the name of the judge, as these records are filed alphabetically.

Safeguards:

These records are maintained in cabinets stored in a locked room.

Retention and disposal:

The personnel section of the folders of United States Supreme Court Judges are sent to National Archives upon the death of the judge. All other sections are retained indefinitely the entire records folders of all other United States Judges.

System manager(s) and address:

Assistant Attorney General, Office of the Legal Policy, United States Department of Justice
10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Address all inquiries to the System Manager. These records will be exempted from subsections (d)(1) and (e)(1) of section 552a, Title 5, United States Code, by the Attorney General under the authority of 5 U.S.C. 552a(k)(5) to the extent therein permitted.

Record access procedures:

A request for access to non-exempt portions of records from this system should be directed orally or in writing to the System Manager. When requests are in writing, the envelope or letter should be marked 'Privacy Access Request.'

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should di

their request to the System Manager, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment(s) to the information.

Record source categories:

Non-exempt sources of information contained in this system include the general public, organizations, associations, the subjects of the records themselves, government agencies appropriate, and other interested parties.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (d)(1) and (e)(1) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/OLP-003

System name:

General Files System of the Office of Legal Policy.

System location:

Office of the Assistant Attorney General, Office of Legal Policy, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

The system encompasses individuals who relate to official Federal investigations, policy decisions, and administrative matters of such significance that the Assistant Attorney General maintains information indexed to the name of that individual, including, but not limited to, subjects of litigation, targets of investigations, Members and staff members of Congress, upper-echelon government officials, and individuals of national prominence or notoriety.

Categories of records in the system:

Records may include case files, litigation materials, exhibits, internal memoranda and records or other records on a given subject or individual. Records vary in number and kind according to the breadth of the Assistant Attorney General's responsibilities (28 CFR 0.23). Records include those of such significance that the Assistant Attorney General has policy or administrative interest, and those which cover investigative or law enforcement cases for which the Assistant Attorney General is asked to provide an analysis and establish future policy direction. A computerized index record containing the subject title and/or individual's name is also maintained.

Authority for maintenance of the system:

These records are maintained pursuant to 5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records may be disclosed to the news media and the public pursuant to 28 CFR unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of privacy.

These records may be disclosed to a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information for investigative or policymaking purposes or to provide constituent assistance.

These records may be disclosed to members of the judicial branch of the Federal Government in response to a specific request where disclosure appears relevant to the authorized functions of the recipient judicial office or court system.

These records may be disclosed to any civil or criminal law enforcement authorities, whether Federal, State, local, or foreign, which requires information relevant to a civil or criminal investigation.

These records may be disclosed to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and

2906.

These records may be disclosed to officials and employees of the White House or any Federal agency which requires information relevant to an agency decision concerning the hiring appointment, or retention of an employee, the issuance of a security clearance, the conduct of a security or suitability investigation, the classifying of a job, or the issuance of a grant or benefit.

These records may be disclosed to Federal, State, and local licensing agencies or associations which require information concerning the eligibility or suitability of an individual for a license or permit.

These records may be disclosed in a proceeding before a court or adjudicative body before which the Office of Legal Policy is authorized to appear when (a) the Office of Legal Policy or any subdivision thereof, or (b) any employee of the Office of Legal Policy in his or her official capacity, or (c) any employee of the Office of Legal Policy in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (d) the United States, where the Office of Legal Policy determines that the litigation is likely to affect it or one of its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the Office of Legal Policy to be arguably relevant to the litigation.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records are stored in paper folders and on index cards. As of August 1982, the index records are also stored on magnetic disks.

Retrievability:

Records may be retrieved by subject title or individual's name.

Safeguards:

Records are maintained in cabinets stored in a locked room or, in the case of those records that are classified, in safes or vaults. The computer is also maintained in a locked room. The computer has a key lock and may be accessed only by persons with a Top Secret clearance and use of a code.

Retention and disposal:

Records are kept indefinitely.

System manager(s) and address:

Deputy Director, Office of Information and Privacy, Office of Legal Policy, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Address all inquiries to the system manager. These records will be exempted from subsections (c)(3) and (4); (d); (e)(1), (2) and (3), (e)(4)(G) and (H), (e)(5); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5).

Record access procedures:

Make requests for access to records from this system in writing to the system manager, clearly mark both the letter and the envelope "Privacy Act Request."

Contesting record procedures:

Make all requests to contest or amend information maintained in the system in writing to the system manager. State clearly and concisely what information is being contested, the reason for contesting it, and the proposed amendment(s) to the information.

Record source categories:

Sources of information contained in this system include individuals, local, State and foreign government agencies as appropriate, the executive and legislative branches of the Federal Government, and interested third parties.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d); (e) and (3), (e)(4)(G) and (H), (e)(5); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(k)(1), (k)(2) and (k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register*. These exemptions apply only to the extent that information in a record pertaining to a particular individual relates to official Federal investigations and law enforcement matters. Those records indexed under an individual's name and which concern policy formulation or administrative matters are not being exempted pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) or (k)(5).

[\[TOP\]](#)

Office of Pardon Attorney

JUSTICE/OPA-001

System name:

Executive Clemency Case Files/Executive Clemency Tracking System.

System location:

Office of the Pardon Attorney (OPA), U.S. Department of Justice, 950 Pennsylvania Ave
Washington, DC. 20530.

Categories of individuals covered by the system:

Individuals who have applied for or been granted executive clemency.

Categories of records in the system:

Paper Files: The system contains the individual case files of persons who have applied for executive clemency, which may include the following: The clemency petition; character affidavits; investigatory material; court-related documents (e.g., presentence reports, judgments of conviction, and court opinions); official court-martial documents (in military cases); prison progress reports and U.S. Parole Commission notices of action; media references (e.g., newspaper and magazine articles); official and other correspondence (both generated and received, whether solicited or unsolicited); and inter-agency and intra-agency reports, recommendations and decisional documents relating to individual clemency matters.

Computerized Records: The system also includes an automated database for tracking the handling of clemency cases from filing to final action. Information used to track such processing may include, but is not limited to, the petitioner's name, social security number, birth date, the date the petition was received, offense and sentencing information, the date of final action by the President, and other case-related information. Clemency case file notes may also be summarized and stored in an automated format, and may include any relevant information that would assist OPA in formulating clemency recommendations to the President or otherwise performing its duties more efficiently.

Authority for maintenance of the system:

The system is established and maintained in order to carry out the duties assigned by the President, pursuant to the power granted him under United States Constitution, Article II, section 2, to the Department of Justice in Executive Order of the President 30-1, dated January 16, 1893; and Executive Order of the President No. 11878 (published at 40 FR 42731), as amended, delegated by the Attorney General to OPA in 28 CFR 0.35 and 0.36 (Attorney General Order No. 1012-83, published at 48 FR 22290), and as described in 28 CFR 1.1 through 1.11 (Attorney General Order No. 1798-93, published at 58 FR 53658; as amended at 65 FR 58223 and 65 FR 58223).

Purpose(s):

Executive clemency case files are maintained by the Attorney General or his designee to facilitate and document the functions of the Attorney General or his designee in receiving, investigating, and evaluating requests for executive clemency; preparing the necessary reports and recommendations from the Department of Justice to the President in clemency matters; serving as liaison with clemency applicants and the public on clemency matters; and ac

the President on the historical exercise of the clemency power. In addition, OPA or the Attorney General may provide other Departmental components records and information from clemency case files to the extent it is necessary to perform their functional responsibilities. For example, following a Presidential decision to grant clemency (and occasionally when clemency is denied), the Department's Office of Public Affairs typically makes appropriate disclosure of information to the public, including the name of the person granted clemency, the date of grant of clemency, the nature of the relief granted (e.g., commutation of sentence, remission of fine, reprieve, or pardon after completion of sentence), the date, sentence, and district court conviction for which clemency was sought, the city and state of the applicant's current place of residence, and the names of his attorney and character affiants, if any. Automated tracking and retrieval systems enhance OPA's ability to maintain and use the information contained in clemency case files.

Routine uses of records maintained in the system, including categories of users and Purposes of Such Uses.

Disclosure of records in the clemency file of an individual who has applied for or been granted clemency, and information contained in such documents, may be made to the following categories of persons when it has been determined by OPA that such a need exists:

- (a) The President, and members of his staff, in order to assist him in the exercise of his constitutional clemency power.
- (b) Current and former government employees, including law enforcement and judicial authorities, whose comments on a particular clemency matter are solicited by OPA in connection with its investigation and review of a case, in order to enable such persons to formulate a response to the request.
- (c) Contractors, grantees, experts, consultants, students, and others performing or working under a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.
- (d) A private contractor or federal agency for the purpose of preparing bound and index volumes containing originals and/or photocopies of the official warrant of clemency granted to each recipient of clemency as a public and official record of Presidential action.

(e) An appropriate federal, state, local, foreign, or tribal law enforcement authority or other appropriate agency charged with the responsibility for investigating or prosecuting a violation of law (whether civil, criminal, or regulatory in nature), in the event the record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law.

(f) A federal, state, local, or tribal agency, including prosecution, corrections, sentencing, parole authorities, in order to assist it in the execution of appropriate actions necessary to implement a Presidential clemency decision or in the performance of its official duties.

(g) A federal, state, local, or tribal agency or regulatory authority where OPA determines the agency requires information relevant to a decision concerning the issuance, renewal, revocation, or suspension of a license, permit, grant, or other benefit, or other need for information in the performance of its official duties.

(h) A court, administrative, or regulatory body when the records, or information derived therefrom, are determined by OPA to be arguably relevant to the litigation or proceeding when one of the following is a party to or has an interest in the litigation or proceeding: (1) OPA; (2) any employee of OPA in his or her official capacity; (3) any employee of OPA in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (4) the United States.

(i) The news media and the public pursuant to 28 CFR 50.2 unless it is determined that disclosure of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(j) A Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

(k) The National Archives and Records Administration and the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(l) A member of the public who has requested information concerning a specific, named individual, provided that such a disclosure shall be limited to: whether a clemency application

been filed, and if so, the date on which it was filed, the type of clemency sought, the office for which clemency is sought, the date and court of conviction, the sentence imposed, the decision of the President to grant or deny clemency and the date of that decision, the administrative closure of a clemency request and the date of such closure.

(m) Former employees of the Department for purposes of: Responding to an official inquiry of a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Data is stored in electronic media via a client/server configuration. Computerized records are stored on hard disk, floppy diskettes, compact disks, magnetic tape, and/or on OPA's local area network. Paper records are stored in individual file folders and a secure file room or cabinets with controlled access, and/or other appropriate GSA approved security containers.

Retrievability:

Individual case files are retrieved primarily by the name of the person who applied for or was granted executive clemency. Case files also may be retrieved by a case file number assigned to each file. Information stored in the computerized case-tracking system is retrieved primarily by searching under the name of the person who applied for or was granted clemency, or whose behalf clemency was sought. Information stored in the computerized case-tracking system may also be retrieved by the clemency case file number, or the applicant's Bureau of Prisons register number (if he was incarcerated at the time he applied for or was granted clemency).

Safeguards:

Paper records are secured through the use of safes, locked file cabinets, and/or restricted access to the space in which they are located. Electronic records are safeguarded in

accordance with DOJ rules and policies governing automated systems security and access, including the maintenance of technical equipment in restricted areas and the required use of individual passwords and user identification codes to access the system.

Retention and disposal:

Individual case files are stored in OPA's work area while the clemency request is pending, generally for up to two years after the date of final decision. Closed case files are transferred to the Washington National Records Center in Suitland, Maryland one full year after the close of the year in which the case was closed. Except for copies of reports furnished to the President for particular clemency matters, clemency warrants and other documents reflecting the President's action in clemency cases, case files in any cases in which clemency is granted, case files in any other cases designated by the Pardon Attorney as having significant public interest, notices issued by OPA to the Office of Public Affairs of the Department of Justice, case files transferred to the Washington National Records Center are destroyed no sooner than 25 years after the case is closed, in accordance with Records Disposition Authority NC1-204-95-1, or successor Records Disposition Authority.

System manager(s) and address:

Pardon Attorney, Office of the Pardon Attorney, U.S. Department of Justice, 500 First Street, NW, Suite 400, Washington, DC 20530.

Notification procedure:

Address inquiries to Office of the Pardon Attorney, U.S. Department of Justice, 950 Pennsylvania Ave., NW., Washington, DC 20530.

Record access procedures:

While the Attorney General has exempted executive clemency case files from the access provisions of the Privacy Act, requests for discretionary releases of records shall be made by writing to the system manager listed above with the envelope and letter clearly marked "Access Request." Include in the request the general subject matter of the document. Provide full name, current address, date and place of birth, signature (which must be either notarized or submitted under penalty of perjury) and a return address for transmitting the information.

Contesting record procedures:

While the Attorney General has exempted executive clemency case files from the correction (contest and amendment) provisions of the Privacy Act, requests for the discretionary correction (contest and amendment) of records should be directed to the system manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it and the proposed amendment to the information sought.

Record source categories:

Sources of information include: individual applicants for clemency, their representatives and persons who write, confer with, or orally advise OPA concerning those applicants; investigative reports of the Federal Bureau of Investigation, the Drug Enforcement Administration, the Internal Revenue Service, and the Immigration and Naturalization Service, and other appropriate government agencies; records of the Bureau of Prisons; reports of the Armed Forces; presentence reports provided by the Bureau of Prisons or the federal Probation Offices; reports of the U.S. Parole Commission; comments and recommendations from current and former federal and state officials; and employees of the Department of Justice and the White House.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3), (c)(4), (d)(1), (d)(3), (d)(4), and (e)(5) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c), and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

Office of Professional Responsibility

JUSTICE/OPR-001

System name:

Office of Professional Responsibility Record Index.

System location:

Office of Professional Responsibility (OPR), U.S. Department of Justice (DOJ), 950 Pennsylvania Avenue NW, Washington, DC 20530.

Categories of individuals covered by the system:

(1) DOJ employees who are the subjects of complaints directed to, or inquiries or investigations conducted by, OPR; (2) individuals (complainants) who write to OPR; (3) individuals (complainants) who write to the Attorney General and other officials of the Department of Justice whose correspondence is referred to OPR; and (4) employees of agencies of the Federal Government, other than DOJ, about whom information indicating possible criminal or administrative misconduct has been developed during the course of routine investigation components of DOJ, when such information is furnished to OPR for referral—if warranted—to an appropriate investigative component of DOJ, or another government agency.

Categories of records in the system:

This system of records consists of complaints filed against DOJ employees, the results of investigations into those complaints, and actions taken after completion of the investigation. This system also includes all records developed pursuant to special assignments given by the Attorney General or the Deputy Attorney General as well as records containing information indicating possible misconduct by employees of the Federal Government other than DOJ, which have been furnished to OPR for referral, if warranted, to the appropriate investigative authority.

Authority for maintenance of the system:

44 U.S.C. 3101 et seq., 28 CFR 0.39 et seq., and Attorney General Order No. 833–79.

Purpose(s):

Information in this system is maintained to provide for the resolution of allegations of misconduct made against Department of Justice employees and to advise complainants of status of investigations and the results.

Routine uses of records maintained in the system, including categories of users and

purposes of such uses:

A relevant record may be disseminated as a routine use of such record as follows: (1) In case in which there is an indication of a violation or a potential violation of law, either on or in connection with other information, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or issued pursuant thereto, the record may be referred to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation or issued pursuant thereto; (2) in the course of investigating the potential or actual violation of law, whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing for such violations, a record may be disseminated to a Federal, State, local or foreign agency, or to an individual or organization if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, trial or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant; (3) a record relating to a case or matter may be disseminated in an appropriate Federal, State, local or foreign court or grand jury proceeding in accordance with established constitutional, substantive or procedural law or practice; (4) a record relating to a case or matter may be disseminated to a Federal, State, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing; (5) a record may be disseminated to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of security clearance or the reporting of an investigation of an employee; (6) information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy; (7) information not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's request when the Member or staff requests information on behalf of and at the request of the individual who is the subject of the record; (8) a record may be disclosed to the National Archives and Records Administration (NARA) in records management inspections conducted under 44 U.S.C. 2904 and 2906; (9) information may be furnished to complainants to the extent necessary to provide such persons with information and explanations concerning the process and/or results of the investigation or case arising from the matters of which they complain and (10) information may be furnished to professional organizations or associations with which individuals covered by this system of records may be affiliated, such as state bar disciplinary authorities, to meet their responsibilities in connection with the administration and maintenance of the system.

of standards of conduct and discipline. (11) relevant information contained in this system records may be disclosed to contractors, grantees, experts, consultants, students, and performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records. (12) relevant and necessary information may be disclosed to former employees of the Department of Justice for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility; (13) relevant information contained in this system of records may be disclosed to a member of the judicial branch of the Federal Government in response to a written request where disclosures are relevant to the authorized function of the recipient judicial office or court system; (14) information in this system may be disclosed to the subject of an investigation or inquiry conducted by OPF to further the investigation or inquiry, or to give notice of the status or outcome of the investigation or inquiry.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information is stored manually in file jackets and electronically in office automation equipment.

Retrievability:

Information is retrieved in most instances by the name of the employee who is the subject of the complaint and in some instances by the name of the complainant.

Safeguards:

The information is stored in safes, locked filing cabinets and office automation equipment in a limited access area and is maintained according to applicable departmental security regulations.

Retention and disposal:

Records in the system are retained and disposed of in accordance with NARA Job # NCI-60-77-6.

System manager(s) and address:

Counsel on Professional Responsibility, Department of Justice, 950 Pennsylvania Avenue
Washington, DC 20530.

Notification procedure:

Address any inquiries to the System Manager listed above.

Record access procedure:

The major part of this system is exempted from this requirement under 5 U.S.C. 552a(j)(k)(1), (k)(2), or (k)(5). To the extent that this system of records is not subject to exemption, it is subject to access and contest. A determination as to exemption shall be made at the time a request for access is received. A request for access to records contained in this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." The request shall include the full name of the individual involved, his or her current address, date and place of birth, notarized signature, together with any other identifying information which may be of assistance in locating the record. The requester will also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what

information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Department officers and employees, and other Federal, State, local and foreign law enforcement and non-law enforcement agencies, private persons, witnesses, and informants.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(4)(G) and (H), (e)(5) and (8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2). In addition, the Attorney General has exempted this system from subsection (d), (e)(1), (e)(4)(G) and (H), and (f) pursuant to 5 U.S.C. 552a (k)(1), (k)(2) and (k)(5). It has been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (d) and has been published in the *Federal Register*.

[\[TOP\]](#)

Office of Public Information

JUSTICE/OPI - 001

System name:

News Release, Document and Index System.

System location:

Room 5114, U.S. Department of Justice, 10th Street and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

A. Defendants in civil and criminal actions brought by the Department of Justice for which releases were issued; B. Current and former employees of the Department of Justice or news releases and biographical information were prepared.

Categories of records in the system:

The system contains an index record of each news release and document issued by the Department of Justice and copies of the news release and document.

Authority for maintenance of the system:

The system is established and maintained at the direction of the Attorney General pursuant to 5 U.S.C. 301 and 44 U.S.C. 3101.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

The index is used to retrieve news releases and documents issued by the Department upon request.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 5 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional.

licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored manually on index cards and letter- and legal-size paper.

Retrievability:

Information is retrieved by using the name of the defendant, subject matter of legal action, state in which action is filed, and name of current or former employee.

Safeguards:

Information contained in the system is unclassified.

Retention and disposal:

The index and one copy of each news release are retained indefinitely. Additional copies are retained for one year and then destroyed.

System manager(s) and address:

Director of Public Information, U.S. Department of Justice, 10th Street and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Same as the above.

Record access procedures:

A request for a copy of a record from this system may be made in writing, by telephone, or by any other means of communication available to any person.

Contesting record procedures:

Persons desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendments to the information sought.

Record source categories:

Sources of information contained in this system are those employees who prepared the document on which a news release is based.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

Parole Commission

JUSTICE/PRC-001

System name:

Docket, Scheduling and Control.

System location:

Records are maintained at each of the Regional Offices for inmates incarcerated in and persons under supervision in each region, except for the National Appeals Board docket maintained in Washington. Duplicates of regional materials are maintained in Washington. Requests for records should be made to the appropriate regional office or Headquarters following addresses: United States Parole Commission, 2nd and Chestnut Sts. Custom House—7th Floor, Philadelphia, PA 19106, United States Parole Commission, 1718 Pennsylvania Avenue, Washington, DC 20006.

St., NW, Suite 250, Atlanta, GA 30309, United States Parole Commission, 5550 Friends Blvd., Chevy Chase Md. 20815, ATTN: National Appeals Board, United States Parole Commission, Air World Center Suite 220, 10920 Ambassador Dr., Kansas City, Mo. 64114, United States Parole Commission, 525 Griffin St., Suite 820 Dallas, Tex. 75202. United States Parole Commission, 1301 Shoreway Road Fourth Floor, Belmont, CA 94002

Categories of individuals covered by the system:

Current and former inmates under the custody of the Attorney General who are to be scheduled for hearings under Commission procedures. Former inmates includes those presently under supervision as parolees or mandatory releasees and those against whom revocation warrant has been issued.

Categories of records in the system:

(a) Docket sheets—Each region and the National Appeals Board in Washington maintain a cumulative series of docket sheets in time sequence showing Commission action. Principal data elements are name and register number of inmate, offense, sentence, and previous present Action. The appeal docket includes the data and type of appeal in addition to the above data. These provide a continual running record of the basic data elements per inmate and former inmate. Docket sheets are used to input this information into a computer program which produces printouts of identical information and certain statistical reports. Hearing schedules—Shortly after inmates are incarcerated, their names appear on an electronic list prepared by the Bureau of Prisons, for initial parole hearings. Following the hearing, the Commission may order that the inmate be denied parole, granted a presumptive parole date, granted an effective (within six months) parole date or continued to a 15 year reconsideration hearing. Other types of hearings and reviews are provided for in the Code of Federal Regulations as part of parole, rescission or revocation procedures. All of the different types of hearings and reviews are placed on schedules for examiners to process when they visit various institutions or hold "local" hearings. The data elements are similar to those on the appeal docket but indicate the number and type of hearing or review to be held instead of the result.

Authority for maintenance of the system:

18 U.S.C. 4201–4218, 5005–5041, 28 CFR part 0, subpart V, and 28 CFR part 2.

Routine uses of records maintained in the system, including categories of users and

purposes of such uses:

(a) The dockets provide the basis of answering basic inquiries, mostly from within the P Commission, as to when a hearing came up for an individual and what action was taken. The schedules indicate to examiners and prison staff the specific hearings and reviews to be prepared for and held.

(b) In the event that material in this system indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute, or regulation, rule or order issued pursuant thereto, the relevant records may be referred to the appropriate agency, whether Federal, State, local or foreign, charged with responsibility for investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

(c) A record from this system of records may be disclosed to a Federal, State or local agency maintaining civil, criminal or other relevant information if necessary to obtain information relevant to an agency decision concerning parole matters.

(d) A record from this system may be disclosed to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

(e) Internal users—Employees of the Department of Justice who have a need to know the information in the performance of their duties.

(f) External users—As noted above, on occasion employees of Federal, State and local law enforcement, correctional, prosecutive, or other agencies, and courts may have access to the information.

Release of information to the news media:

Information permitted to be released to the news media and the public pursuant to 28 C.F.R. 50.2 may be made available unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to members of congress.

Information not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and in response to a communication from an individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA):

A record may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information stored in the system is on sheets of paper, one item per line, stored in folder binders. An experimental program to store such data on tape disk, or microfiche using laser technology, and to prepare certain computer printouts is in effect in all regions. Data also may be stored on paper printouts through file retention.

Retrievability:

Name, register number, date, institution Commission action, and statistical data as to such actions.

Safeguards:

Copies of dockets, printouts and schedules are not disseminated outside of Commission offices and Bureau of Prisons installations. They are available only to Commission and Bureau of Prisons employees on a "need to know" basis. Information therefrom may be given outside the Department as indicated in the "Routine Uses." If so, a letter will be written covering the disclosure, date and identity of the recipient. If information must be given over the phone in an emergency, the caller will be identified beforehand and details of the call recorded.

Retention and disposal:

Records in this system are kept for five (5) years after the effective date of the schedule of the last item recorded on the docket. They are then shredded and electronically stored records are erased.

System manager(s) and address:

Director, Research and Program Development, United States Parole Commission, 5550 Friendship Blvd., Chevy Chase, MD 20815.

Notification procedure:

Address inquiries to Regional Commissioner at appropriate location. For general inquiries, address system manager. The Attorney General has exempted this system from compliance with the provisions of subsection (d), under the provisions of subsection (j).

Record source categories:

(1) Bureau of Prisons files; (2) Parole Commission and Bureau of Prison's employees; (3) Records; (4) Parole Commission inmate files.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(3), (e)(4)(G) and (H), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/PRC-003

System name:

Inmate and Supervision Files.

System location:

Records are maintained at each of the U.S. Parole Commission's (USPC) Regional Office inmates incarcerated in and persons under supervision in each region. Records are housed temporarily at the Commission's Headquarters Office located at 5550 Friendship Blvd., Wood Chase, MD 20815 when used by the National Appeals Board or other Headquarters personnel. A duplicate records of certain data elements from files is maintained on microfiche for Headquarters use. Prior to the first parole hearing, the inmate's file is maintained at the institution at which he is incarcerated. Certain records on parolees and mandatory releasees are maintained at probation offices. All requests for records should be made to the appropriate regional office at the following addresses: U.S. Parole Commission, Customs House Station, 5th Floor, Second and Chestnut Streets, Philadelphia, Pa. 19106. U.S. Parole Commission, Peachtree St. NW, Suite 250, Atlanta, GA 30309. U.S. Parole Commission, Air World Center, Suite 220, 10920 Ambassador Drive, Kansas City, Mo. 64153. U.S. Parole Commission, Griffin St., Suite 820, Dallas, Tex. 75202, U.S. Parole Commission, 1301 Shoreway Road, 2nd Floor, Belmont, CA 94002.

Categories of individuals covered by the system:

Current and former inmates under the custody of the Attorney General. Former inmates include those presently under supervision as parolees or mandatory releasees.

Categories of records in the system:

1. Compulation of sentence and supportive documentation.
2. Correspondence concerning pending charges, and wanted status, including warrants.
3. Requests from other Federal and non-Federal law enforcement agencies for notification.

to release.

4. Records of the allowance forfeiture, withholding and restoration of good time.

5. Information concerning present offense, prior criminal background sentence, and par from the U.S. Attorneys, the Federal Courts, and Federal prosecuting agencies.

6. Identification data.

7. Order of designation of institution or original commitment.

8. Records and reports of work and housing assignments.

9. Program selection assignments and performance adjustments/progress reports.

10. Conduct records.

11. Social background.

12. Educational data.

13. Physical and mental health data.

14. Parole Commission applications, appeal documentation, orders actions, examiner's summaries, transcripts or tapes of hearings, guideline evaluation documents, parole or mandatory release certificates, statements or third parties for or against parole, special on youthful offenders and adults required by statute and related documents.

15. Correspondence regarding release planning, adjustment and violations.

16. Transfer orders.

17. Mail and visit records.

18. Personal property records.

19. Safety reports and rules.
20. Release processing forms and certificates.
21. Interviews requests forms from inmates.
22. General correspondence.
23. Copies of inmate court petitions and other court documents.
24. Report of probation officers. Commission correspondence with former inmates and c and Commission order and memoranda dealing with supervision and conditions of paro mandatory release.
25. If an alleged parole violation exists, correspondence requesting a revocation warrant warrant application, warrant, instructions as to service, detainers and related documents

Authority for maintenance of the system:

18 U.S.C. 4201–4218, 5005–5041, 28 CFR part 0, subpart V, and 28 CFR part 2.

Purpose(s):

The system constitutes the agency's records upon which it bases all its decisions with r to every stage of parole consideration from initial hearing to termination of parole superv For example, it is used by USPC hearing examiners to perform a prehearing review and conduct the inmate's initial parole hearing. After that hearing, it is maintained in the app regional office where it provides the principal information source for all decisions leading parole or denial of parole, and all decisions following release to supervision. It is used a headquarters when appeals come before the National Appeals Board or when needed t counsel and others on the headquarters staff. It is used by employees at all levels, inclu USPC members, to provide information for decisionmaking in every area of USPC responsibility. Files of released inmates are used to make statistical studies of subjects to parole and revocation. Finally, the file is maintained to provide the rationale of USPC when an agency determination is questioned by members of the public or challenged in judicial proceedings.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

- (a) The system may be used as a source for disclosure of information which is solely a matter of public record and which is traditionally released by the agency to further public understanding of its criminal justice system, including but not limited to offense, sentencing data, and prospective release date.
- (b) The system may be used to provide an informational source for responding to inquiries from Federal inmates, their families, representatives, and Congressional offices.
- (c) Record from the system of records may be routinely disclosed to U.S. Probation Officers for the performance of their official duties.
- (d) In the event that the USPC is informed of a violation or suspected violation of law whether civil, criminal or regulatory in nature, and whether arising by general statute, or by regulation or rule or order issued pursuant thereto, the relevant records may be disclosed to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or regulation or order, issued pursuant thereto.
- (e) Records from this system may be disclosed to a Federal, State or local agency or court that agency or court requests information for an official purpose to which the documents appear to be relevant.
- (f) A record from this system may be disclosed to a person or to persons who may be exposed to harm through contact with a particular parolee or mandatory releasee (or to persons in a position to prevent or minimize such harm), if it is deemed to be necessary to give notice that such danger exists.
- (g) Lists of names of parolees and mandatory releasees entering a jurisdiction and related information may be disclosed to law enforcement agencies upon request as may be required for the protection of the public for the enforcement of parole conditions.
- (h) Disclosure of USPC notices of action may be made (1) by the Office of Public Affairs of the U.S. Department of Justice to the public generally, and (2) by USPC to specific crime victims.

and witnesses (as those terms are used in the Victim and Witness Protection Act of 1980) in the files of prisoners whose applications for parole have been decided by USPC. The purpose of such disclosure is to further understanding of the criminal justice system by the public and by crime victims and witnesses.

(i) Incidental disclosure of file material may be made during the course of a parole or parole revocation hearing to victims and witnesses of crime and other legitimately interested persons authorized by USPC to attend such hearing, so as to further their understanding of the decision and permit their intelligent comment with respect to USPC's decision.

(j) Records which are arguably relevant to litigation in which the Parole Commission has an interest, or to the litigation defense of its present or former employees (if the Department of Justice has agreed to provide representation) may be disclosed from a current or former inmate's or parolee's file by disseminating in proceeding before a court or tribunal at a time deemed appropriate by the Government's attorney.

(k) A record from this system of records may be disclosed to a current or former criminal justice official who is a defendant in a lawsuit brought by, or which involves, an individual who is the subject of a file maintained in this system of records, provided that such litigation arises from allegations of misconduct on the part of the defendant while a criminal justice official, and the records are arguably relevant to the matter in litigation. Such records may be disclosed to the defendant to facilitate the preparation of his or her defense.

(l) Records from this system may be disclosed to any person performing any service for USPC pursuant to authority exercised by the Chairman under 18 U.S.C. 4204(b)(1) through (8), and for the purposes contemplated by that statute.

(m) A record relating to the identification and location of Human Immunodeficiency Virus (HIV)-positive parolees (those who test positive for the Acquired Immune Deficiency Syndrome virus) may be disseminated to State or local health departments where permitted by State law.

(n) Where the Commission or supervising probation office believes that a specific person has been exposed to a medically recognized risk from an HIV-positive parolee and has been advised of such risk, a record relating to the identification of that parolee may be released to the parolee's physician or State or local health authorities for the purpose of determining if the physician or health authorities are willing to provide a warning to the third-party at risk, if willing, for the purpose of providing such a warning.

(o) A record relating to the identification of an HIV-positive parolee may be made to a third party where it is believed that such third party is or has been exposed to medically recognized risk from an HIV-positive parolee and has not been advised of such risk. Such disclosure under this routine use would be made only where the parolee's physician or State or local health authorities are unable or unwilling to make such a warning to the third party; such disclosures will be made discretely and as a confidential communication.

(p) To the extent not prohibited by State law, a record relating to the identification and location of an HIV-positive parolee may be disseminated to those medical facilities, State or local health departments, community organizations or similar groups capable of providing medical health counseling to HIV-positive parolees.

(q) A record relating to the identification of an HIV-positive parolee may be released to the United States Marshal when the Commission issues a parole violator warrant for the arrest of an HIV-positive parolee.

(r) Information permitted to be released to the news media and the public pursuant to 28 U.S.C. 50.2 may be made available unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(s) Information not otherwise required to be released pursuant to 5 U.S.C. 552 may be released to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

(t) A record may be disclosed to the National Archives and Records Administration and the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Manual requests records are stored in locked safes. Automated requests records are stored on disks.

Retrievability:

Requests reports are filed and retrieved under the names of those persons and individuals identified under the caption "Categories of individuals covered by the system." These records are retrieved by Department personnel to perform their duties, e.g., when subsequent requests are made by the public for copies of their previous requests and responses thereto, or when the requester submits a supplemental request to information clarifying a previous request.

Safeguards:

Access to requests records is limited to Department of Justice personnel who have need for these records to perform their duties. Request files (manual records) are stored in locked safe drawers. Automated records are stored in an office which is occupied during the day and locked at night.

Retention and disposal:

Records are held at the regional office until termination of sentence then transferred to the Washington National Records Center. Records are destroyed ten years after the case becomes inactive.

System manager(s) and address:

FOIA Officer, United States Parole Commission, 5550 Friendship Blvd., Chevy Chase, MD 20815.

Notification procedure:

Address inquiries to Regional Commissioner at appropriate location. For general inquiries, address System Manager. The Attorney General has exempted this system from compliance with the Freedom of Information Act.

with the provisions of Subsection (d) under the provisions of Subsection (j).

Record source categories:

1. Individual inmate; 2. Federal law enforcement agencies and personnel; 3. State and probation services; 4. Non-Federal law enforcement agencies; 5. Educational institution; 6. Hospital or medical sources; 7. Relatives, friends and other interested individuals or groups in the community; 8. Former or future employers; 9. Evaluations, observations, reports and findings of institution supervisors, counselors, boards and committees, Parole Commission examiners, Parole Commission Members; 10. Federal court records; 11. U.S. Bureau of Prisons personnel and records.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c) (3) and (4), (d)(e) (3), (e)(4) (G) and (H), (e)(8) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). The exemptions have been promulgated in accordance with the requirements of U.S.C. 553 (b), (c) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/PRC-004

System name:

Labor and Pension Case, Legal File and General Correspondence System.

System location:

All Labor and Pension cases, most legal files and some general correspondence material are located at: Commission Headquarters, 5550 Friendship Blvd., Chevy Chase, MD 20815. The balance of the general correspondence material is located at the Commission's Regional Offices, the addresses of which are specified in the Inmate and Supervisions System.

Categories of individuals covered by the system:

All applicants for exemptions under 29 U.S.C. 504 and 29 U.S.C. 1111, all persons litigating

with the U.S. Parole Commission, all persons corresponding with the Commission on subjects not amenable to being filed in an inmate or supervision file identified by an individual, and all correspondence from Congressmen inquiring about constituents.

Categories of records in the system:

Pursuant to 29 U.S.C. 504 and 1111, the Commission processes applications of persons convicted of certain crimes for exemptions to allow their employment in the Labor or public plan fields. The files contain memoranda, correspondence, and legal documents with information of a personal nature, i.e., family history, employment history, income and wealth, etc., and of a criminal history nature, i.e., record of arrests and convictions, and details of the crime which barred employment. The final decision of the Commission in each case is a public document under the Freedom of Information Act. The General Counsel's Office and the Parole Commission maintains work files for each inmate or person on supervision who is litigating with the Commission. These files contain personal and criminal history type data regarding inmates, and internal communications among attorneys, Commissioners and staff in developing the Commission's legal position in these cases. Files of the Commission's correspondence with Congressmen who inquire about constituents who have paroles or parole revocations pending or other subjects are maintained in the Chairman's Office and in the regional offices. Files of correspondence, notes, and memoranda concerning parole revocation, rescission, and related problems are also maintained in those locations. Some of this material duplicates material in the inmate files and contain criminal history type information about individuals.

Authority for maintenance of the system:

These files are maintained pursuant to 18 U.S.C. 4201, 5005–5041, 28 CFR part O, subpart O, 28 CFR parts 2 and 4, 29 U.S.C. 504, 1111, and all statutory sections and procedural rules allowing inmates, persons under supervision, or others to litigate with the Parole Commission.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Within the Parole Commission material in this system is used respectively by General Counsel's Office staff and Commission Members in processing exemption applications. Legal file material is used by General Counsel's Office staff in asserting the litigative position of the Commission. The general correspondence is used by the Commission personnel in

responding to Congressmen, and by Commission Members and others in transacting the day-to-day business of the Commission. Final pension and labor case decisions are used by the Commission, the Justice, and Labor Departments, and the public to establish precedent in this field of administrative law.

In the event that material in this system indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute, or regulation, rule or order issued pursuant thereto, the relevant records may be referred to the appropriate agency, whether Federal, State, or local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto. A record from this system of records may be disclosed to a Federal, State or local agency maintaining civil, criminal or labor records relevant information if necessary to obtain information relevant to an agency decision regarding pension or labor matters. A record from this system may be disclosed to a Federal agency in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

Release of information to the News Media:

Information permitted to be released to the news media and the public pursuant to 28 C.F.R. 50.2 may be made available from systems of records maintained by the U.S. Parole Commission unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress:

Information contained in systems of records maintained by the U.S. Parole Commission and otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and in response to a communication from the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA):

A record may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

All data is on documents or other papers on bound files. Labor and pension case material is in the General Counsel's Office or the Chairman's Office at Headquarters, except for final decisions which are in the Freedom of Information Act reading room. Legal files are in the General Counsel's Office at Headquarters. General correspondence is in the Chairman's Office, the office of his staff at Headquarters, and the offices of each Regional Commissioner.

Retrievability:

Labor, pension, and legal file material is indexed or filed by name of applicant or litigant respectively. General correspondence is indexed or filed by subject, time sequence or individuals to whom the item refers.

Safeguards:

Material is available only to Commission employees on a "need to know" basis. Storage locations are supervised by day and locked at night. Only disclosure made therefrom is to other agencies of the Department of Justice, the U.S. Probation Office, Federal enforcement agencies or the Congress. Disclosure to congressmen in response to inquiries concerning constituents is subject to the exemptions of the Freedom of Information Act. The Commission's decisions in labor and pension cases are public information under the Freedom of Information Act.

Act.

Retention and disposal:

Records are maintained for 10 years after the fiscal decision of the court, and are shredded electronically thereafter.

System manager(s) and address:

General Counsel, United States Parole Commission, 5550 Friendship Blvd., Chevy Chase, MD 20815.

Record source categories:

a. Applicants for exemptions under 29 U.S.C. 504 and 29 U.S.C. 1111; b. U.S. Department of Labor; c. Administrative Law Judges and others connected with labor or pension cases; d. Litigants proceeding against Parole Commission; e. The Commission's legal staff and other Commission personnel; f. Congressmen and others making inquiries of Commission; g. Commission Members and employees responding to inquiries, corresponding with other agencies, preparing speeches, policy statements and other means of contact with other branches of Federal Government, State, and local governments, and the public.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(3), (e)(4) (G) and (H), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(3). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/PRC-005

System name:

Office Operation and Personnel System.

System location:

At each regional office as indicated in the "Inmate and Supervision File System Report" the U.S. Parole Commission, 5550 Friendship Blvd., Chevy Chase, MD 20815.

Categories of individuals covered by the system:

Present and former Commission Members and employees of the U.S. Parole Commission

Categories of records in the system:

Personnel records, leave records, property schedules, budgets and actual expense figures, obligation schedules, expense and travel vouchers, and the balance of the usual paper run a Government office efficiently.

Authority for maintenance of the system:

All statutory sections, CFR sections, and OPM, MSPB, GSA, and OMB directives establish procedures for government personnel, financial, and operational functions.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Day-to-day activity involving personnel, financial, procurement, maintenance, recordkeeping, mail delivery, and management functions.

Release of information to the News Media:

Information permitted to be released to the news media and the public pursuant to 28 C.F.R. 50.2 may be made available from systems of records maintained by the Department of Justice, unless it is determined that release of the specific information in the context of a particular request would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress:

Information contained in systems of records maintained by the U.S. Parole Commission

otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and in response to a communication from the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA):

A record may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records are in paper files or on computer printouts. They are stored in operations areas and offices.

Retrievability:

Data of a personal nature is in employee personnel files, used by Commission personnel on a "need to know" basis. Each employee has a right to access his own file on request. Other files are used by Commission personnel on a "need to know" basis.

Safeguards:

Files are supervised by appropriate personnel during the working day and are locked in

at night.

Retention and disposal:

Cutoff files at the end of the calendar year, held at the agency for one year then transfer to the Washington National Records Center. Destroy seven years after cutoff.

System manager(s) and address:

Executive Officer, U.S. Parole Commission, 5550 Friendship Blvd., Chevy Chase, MD 20815

Notification procedure:

Same as the above.

Record access procedures:

Same as the above.

Contesting record procedures:

Same as the above.

Record source categories:

The U.S. Parole Commission, the Justice Management Division and all other contributing government agencies.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/PRC-006

System name:

Statistical, Education and Developmental System.

System location:

Parole Commission Headquarters, 5550 Friendship Blvd., Chevy Chase, MD 20815.

Categories of individuals covered by the system:

Any inmate or former inmate under custody of the Attorney General including former inmates supervised as parolees or mandatory releases.

Categories of records in the system:

All records as described in the Workload Record, Decision Result, and Annual Report S Plus data on additional input forms and certain follow-up forms and the Salient Factor Worksheet Form. These forms include criminal history-type data elements regarding specific individuals selected from the above category of individuals. This data is either organized, processed by hand or is input into a computer and has been used to provide the following one-time reports in pamphlet-text form: (a) Administrative Review of Parole Selection and Revocation decisions; (b) Parole Decisionmaking, a Salient Factor Score; (c) Effect of Representation at Parole Hearings; (d) Parole Decisionmaking—Structuring Discretion (Served and Release Performance—A Federal Sample and certain additional reports, all available in the public reading room. The data base collected as described in this and in JUSTICE/PRC 007 system will be used to prepare studies on similar or related subjects in the future. It has been used to develop revocation guidelines similar to parole guidelines, rescission guidelines and other operational improvements. Items collected for this data may change depending on the subject matter of new studies to be undertaken by the Commission.

Authority for maintenance of the system:

18 U.S.C. 4201–4218, 5005–5041, 28 CFR part O, subpart V, 28 CFR part 2.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

a. Internal—Develop methodology for a more scientific determination of parolability and

revocability, methodology to comply with changing concepts of due process, and methods to select persons to be released from prison who will be less likely to recidivate.

b. External—Add to the general body of knowledge in the parole area of criminology, and provide educational material for other parole boards, and members of the criminal justice academic communities interested in this subject. Published pamphlets in text form are prepared on subjects of interest in this area of criminology and are circulated freely. They contain no references to individuals, either by name, address, register number or other means of identification. They do not contain recognizable fact situations, descriptions, or other information through which identification of any individual within the present or former jurisdiction of the Parole Commission can be made.

Release of information to the news media:

Information permitted to be released to the news media and the public pursuant to 28 C.F.R. 502 may be made available from systems of records maintained by the U.S. Parole Commission unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to members of congress:

Information contained in systems of records maintained by the U.S. Parole Commission otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and in response to a communication from the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA):

A record may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional

licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Data is in input forms on printouts or other computer produced storage media. It is stored as described in the JUSTICE/PRC-007 system description. Pamphlet text reports are public documents stored in offices, libraries, and in bookshelves, and in the public reading room.

Retrievability:

Information by name, register number or FBI identification number may be retrieved from input forms, card decks, or storage media. This material is used only by authorized Parole Commission personnel on a "need to know" basis and is data processed only by authorized Bureau of Prisons or Justice Department personnel. Material is not retrieved in identifiable form except that computer produced "hard copy" may be used to prepare a report or internal papers. The final pamphlet text reports and material resulting from studies are used by Parole Commission personnel for internal purposes and the public externally. None of this material contains any references to an individual. Documents which contain information concerning one individual are made available to that individual if requested under the Privacy Act.

Safeguards:

See "Safeguards" section of JUSTICE/PRC-007 regarding input forms, printouts, discs, tape. Reports in pamphlet form are not safeguarded.

Retention and disposal:

See "Retention and Disposal" of preceding system. The studies in pamphlet form are not disposed of on schedule. Some will be maintained perpetually in archives.

System manager(s) and address:

Research Director, U.S. Parole Commission, 5550 Friendship Blvd., Chevy Chase, Md.

Record source categories:

a. Commission inmate files; b. Docket Sheets; c. Commission Notices of Action, orders and documentation following hearings; d. Commission warrant applications and warrants; e. General Commission records and data; f. Enforcement agency records regarding former inmates.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(4) (G) and (H), (e)(8), (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 553. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/PRC-007

System name:

Workload Record, Decision Result, and Annual Report System.

System location:

U.S. Parole Commission Headquarters, 5550 Friendship Blvd., Chevy Chase, MD 20815

Categories of individuals covered by the system:

Any inmate and parolee or mandatory releasee who has been the subject of a decision period covered in the report for which the data is used (prior month, prior quarter, prior year, or other period).

Categories of records in the system:

Certain original input forms indicate the inmate or person under supervision by name and

register number and give the date and specific statistical detail as to the decision made. include criminal history type of information regarding the persons in questions. The prin types of decisions covered are after initial or review hearings, after a record review, after Regional Appeal, after National Appeal, and after a decision reopening and modifying. data is input into a computer and is used to provide the following: (a) A monthly report c workload containing number and type of hearings per region further broken out by insti within regions and type of sentence; (b) Bimonthly report on decision results indicating, other statistics, number and type of decisions within above, and below guidelines broke by examiners making the decisions; (c) Other or substitute reports as needed; and (d) Together with land posted data on other items of statistical value, this data is being use create the Annual Report of the Commission.

Authority for maintenance of the system:

18 U.S.C. 4201–4216, 5005–5041, 28 CFR part O, subpart V, 28 CFR part 2

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

- (a) These records are used internally to analyze work product, the performance of evalu and various types of procedures and hearings and to evaluate the guidelines and other Commission procedures.
- (b) These records are used to prepare an annual report to the Attorney General, and Co and the public indicating in quantitative and qualitative terms Commission activity and accomplishment.
- (c) In the event that material in this system indicates a violation or potential violation of l; whether a civil, criminal or regulatory in nature, and whether arising by general statute, regulation, rule or order issued pursuant thereto, the relevant records may be referred t appropriate agency, whether Federal, State, local, or foreign charged with the responsil investigating or prosecuting such violation or charged with enforcing or implementing th statute, rule, regulation or order issued pursuant thereto.
- (d) A record from this system of records may be disclosed to a Federal, State, or local a maintaining civil, criminal or other relevant information if necessary to obtain information relevant to Parole Commission matters.

(e) A record from this system may be disclosed to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that information is relevant and necessary to the requesting agency's decision on the matter.

Release of Information to the News Media:

Information permitted to be released to the news media and the public pursuant to 28 C.F.R. 50.2 may be made available from systems of records maintained by the U.S. Parole Commission unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of Information to Members of Congress:

Information contained in the systems of records maintained by the U.S. Parole Commission, otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and in response to a communication from the individual who is the subject of the record.

Release of information to the National Archives and Records Administration (NARA) and General Services Administration (GSA):

A record may be disclosed as a routine use to the NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of

in the system:***Storage:***

Paper input forms are stored in folders only until information from them is entered into readable media. Monthly and other reports in the form of computer printouts are filed in folders. Annual report is in book form and stored in library shelves.

Retrievability:

Data in this system can be retrieved by inmate's name and register number from the original input forms, and computer-produced storage media. It is usually only retrieved by regional examiner, by type of decision made or hearing held, by relation to the guidelines and other similar means except for individual case retrievability when infrequently required.

Safeguards:

Data on forms, tape or other computer produced storage media retrievable by individual is stored in the Commission's Office in cabinets. Commission employees supervise this data day and use it on a "need to know" basis. The rooms where it is stored are locked outside office hours and the entire Headquarters building is locked at certain times with card key access. Monthly and other reports are for use of the Chairman, the Executive Officer and Commission Members and professional personnel. No information thereon is retrievable pertaining to any individual except certain breakouts by Parole Commission employee examiners and by inmate in the guideline section of reports. These printouts are stored in Commission Headquarters offices, all of which are supervised by day, and locked at night. Annual Report contains no information identifiable by individual and is a public document.

Retention and disposal:

The master file and documentation are to be retained permanently. All other related records including reports and software, are to be destroyed when no longer needed for administrative use.

System manager(s) and address:

Director, Research and Program Development, 5550 Friendship Blvd., Chevy Chase, MD 20815.

Record source categories:

(a) Commission inmates files; (b) Docket sheets; (c) Commission notices of action, order documentation following hearings; (d) Commission warrant applications and warrants; (e) General Commission records and data.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(3), (e)(4) (G) and (H), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (3) and have been published in the *Federal Register*.

[\[TOP\]](#)

Office of Special Counsel for Immigration-Related, Unfair Employment Practices

JUSTICE/OSC-001

System name:

Central Index File and Associated Records, JUSTICE/OSC-001.

System location:

U.S. Department of Justice, Special Counsel for Immigration Related Unfair Employer Practices (OSC), 1100 Connecticut Avenue, NW, Washington, DC 20036 and Federal E-Verify Center, Suitland, Maryland 20409.

Categories of individuals covered by the system:

These persons may include: Subjects of investigations, victims, potential witnesses and representatives on behalf of individuals and other correspondents on subjects directed or referred to OSC in potential or actual cases and matters of concern to OSC.

Categories of records in the system:

The system consists of (1) alphabetical indices bearing names of the individuals identified

above and (2) the associated record to which the indices relate containing the general and particular records of all OSC correspondence, cases, matters, and memoranda, including but not limited to investigative reports, correspondence to and from OSC, internal memoranda, legal papers, evidentiary materials and exhibits.

Authority for maintenance of the system:

44 U.S.C. 3101; 8 U.S.C. 1324b; and 29 CFR part 44.

Purpose(s):

This system has been established to maintain investigatory and law enforcement record concerning charges filed with OSC by or on behalf of individuals alleging immigration-related employment discrimination. The system also contains charges filed with other law enforcement entities that have been referred to OSC pursuant to section 102 of the Immigration Reform and Control Act of 1986 (8 U.S.C. 1324b) to provide relief for injured parties and to enforce prohibition of immigration-related, unfair employment practices.

Employees and officials of the Department may access the system to make decisions in the course of investigations and legal proceedings; to assist in preparing responses to correspondence from persons outside the Department; to prepare budget requests and reports on the work product of OSC; and to carry out any other authorized internal duties.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

(1) A record relating to a possible or potential violation of law may be disseminated to the appropriate Federal, State or local agency charged with the responsibility to enforce or implement such law; (2) in the course of an investigation or litigation of a case or matter, a record may be disseminated to a Federal, State or local agency, or to an individual or organization, if there is reason to believe that such agency, individual or organization possesses information or has the expertise in an official or technical capacity to analyze information relating to the investigation, trial or hearing and the dissemination is reasonably necessary to elicit such information or expert analysis or to obtain the cooperation of a prospective witness or informant; (3) a record relating to a case or matter, or any facts derived therefrom, may be disseminated in a proceeding before a court or adjudicative body before which OSC is authorized to appear, when the United States, or any agency or subdivision

thereof, is a part of litigation or has an interest in litigation and such records are determined by OSC to be arguably relevant to the litigation; (4) a record relating to a case or matter may be disseminated to an actual or potential party of litigation or the party's attorney (a) to negotiate or discuss such matters as settlement of the case or matter or (b) to conduct a formal or informal discovery proceeding; (5) a record relating to a case or matter that has been referred to OSC for investigation may be disseminated by OSC to referring agencies to notify such agency of the status of the case or matter or of any determination that has been made; (6) a record may be disseminated to the United States Commission on Civil Rights in response to a request and pursuant to 42 U.S.C. 1975d; (7) information permitted to be released to the media and the public pursuant to 28 CFR 50.2 may be made available unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy; (8) information in the system may be disclosed if necessary to respond to inquiries by Members of Congress on behalf of individual constituents that are subjects of OSC records; and (9) records may be disclosed to the National Archives and Records Administration and to the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information in this system is indexed, and stored in file jackets and on computer disks or

Retrievability:

Entries are arranged alphabetically and are retrieved from the computer by names of the individuals covered by this system of records. Information may also be retrieved from file jackets by an assigned number appearing in the manual index.

Safeguards:

Information in manual and computer form is safeguarded and protected in accordance with applicable Department security regulations for systems of records. Only those employees with the need to know in order to perform their duties will be able to access the information. Access to records in the computer system is restricted through use of password encryption. Access to both the manual and computer system is restricted by locks on storage facilities.

Retention and disposal:

Records are maintained in the system while current and required for official Government business. When no longer needed on an active basis, the paper files are transferred to the Federal Records Center, Suitland, Maryland, and some records are transferred to computer tape and stored in accordance with Departmental security regulations for systems of records. A request for Records Disposition Authority is pending approval of the National Archives and Records Administration.

System manager(s) and address:

Special Counsel for Immigration Related Unfair Employment Practices, U.S. Department of Justice, Post Office Box 65490, NW, Washington, DC 20035.

Notification procedure:

Address inquiries to the System Manager listed above.

Record access procedures:

Part of this system is exempted from this requirement under 5 U.S.C. 552a(k)(2). To the extent that this system of records is not subject to exemption it is subject to access and contestation. Determination as to exemption shall be made at the time a request for access is received. A request for access shall be made in writing, with an envelope and letter clearly marked "Access Request." Include in the request the full name of the individual, his or her current address, date and place of birth, notarized signature (28 CFR 16.41(b)), the subject of the case or matter as described under "categories of records in the system," and any other information which is known and may be of assistance in locating the records, such as the name of the immigration-related employment discrimination case or matter involved, wh

when the discrimination occurred, and the name of the judicial district involved. The request will also provide a return address for transmitting the information. Access request should be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information.

Record source categories:

Sources of information contained in this system include the individual covered by the system and may include any agency or person who has provided (or has offered to provide) information related to the law enforcement responsibilities of OSC.

Systems exempted from certain provisions of the act:

The Attorney General has exempted parts of this system from subsections (c)(3) and (d) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/OSC-003

System name:

Special Counsel for Immigration Related Unfair Employment Practices Travel Reports, JUSTICE/OSC-003.

System location:

U.S. Department of Justice, Special Counsel for Immigration Related Unfair Employer Practices (OSC), 1100 Connecticut Avenue, NW, Washington, DC 20036.

Categories of individuals covered by the system:

All persons who have filed travel authorization forms or travel voucher forms for official travel on behalf of OSC.

Categories of records in the system:

The system contains information concerning travel expenditures recorded on travel authorization forms (DOJ-501) and travel voucher forms (SF-1012) by OSC employees and other persons authorized to travel for OSC and submitted to the Executive Office of OSC.

Authority for maintenance of the system:

44 U.S.C. 3101; 8 U.S.C. 1324b; and 28 CFR part 44.

Purpose(s):

This system enables OSC to ensure authorized travel, account for its travel expenditure and manage the appropriated funds therefor. It also permits OSC to maintain account balances and properly reimburse those who travel on behalf of OSC.

Department employees may access the system to make reports to the Executive Office, for its use in reviewing and controlling OSC expenditures. Employees may also access the system to process travel authorizations and reimbursements for travel.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

(1) A record relating to a case or matter, or any facts derived therefrom, may be disseminated in a proceeding before a court or adjudicative body before which OSC is authorized to appear when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by OSC to be arguably relevant to the litigation; (2) a record relating to a case or matter may be disseminated to an actual or potential party to litigation or the party's attorney (a) to negotiate or discuss such matters as settlement of the case or matter or (b) to conduct a formal or informal discovery proceeding; (3) information permitted to be released to the news media and the public pursuant to 28 C.F.R. 16.101.

50.2 may be made available unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy. (4) information may be disclosed as is necessary to respond to inquiries by Members of Congress on behalf of individual constituents that are subjects of OSC records; and (5) information may be disclosed to the National Archives and Records Administration and to the General Services Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Travel data are stored on computer disks. Individual vouchers and travel authorization forms are stored in file jackets.

Retrievability:

Records are retrieved by the names of those individuals covered by this system of records.

Safeguards:

Information in manual and computer form is safeguarded and protected in accordance with applicable Department security regulations for systems of records. Only those employees with the need-to-know in order to perform their official duties will be able to access the stored information. Access to the records in the computer system is restricted by the locks on server facilities.

Retention and disposal:

Records are maintained in the system while current and required for official Government use. When no longer needed on an active basis, the records are transferred to computer tape and stored in accordance with Departmental security regulations for systems of records. Final disposition is in accordance with General Records Schedule 9, items 3, 4 and 5.

System manager(s) and address:

Special Counsel for Immigration Related Unfair Employment Practices, U.S. Department of Justice, Post Office Box 65490 NW, Washington, DC 20035.

Notification procedure:

Same as above.

Record access procedures:

Requests for access to records should be directed to the System Manager listed above. Mark the envelope and letter "Privacy Access Request;" provide the full name and notarial signature of the individual who is the subject of the record, his/her date and place of birth, any other identifying number or information which may assist in locating the record; and a return address.

Contesting record procedures:

Individuals desiring to contest or amend information should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information.

Record source categories:

Sources of information contained in this system are OSC employees and other persons authorized to travel on behalf of OSC and who file travel authorization and travel voucher forms.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

Office of Special Counsel—Waco

OSCW-001

System name:

CaseLink Document Database for Office of Special Counsel—Waco.

Security classification:

Unclassified.

System location:

Office of Special Council-Waco, 200 N. Broadway, 15th Floor, St. Louis, Missouri 63102

Categories of individuals covered by the system:

Individuals who are referenced in documents collected or created by the Office of Special Counsel, relating to the investigation of the events occurring in Waco, Texas on April 19

Categories of records in the system:

The system contains documents produced by other federal agencies in response to requests from this office, court records (such as briefs, motions, transcripts from grand jury testimony and orders), inter-agency and intra-agency correspondence, legal research, and other records and documents. These documents include civil investigatory and/or criminal law enforcement information. Finally, the system includes memoranda of interviews (MOIs) conducted by OSC.

Authority for maintenance of the system:

The system was established and is maintained pursuant to 5 U.S.C. 301, 44 U.S.C. 3101, 28 U.S.C. 509 and 510.

Purpose(s):

The purpose of this system is to maintain all documents collected by the Office of Special Counsel (OSC) as well as all the memoranda of interviews conducted by the OSC during inquiry into government conduct relative to certain events occurring in Waco, Texas.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information contained in the system, including the memoranda of interviews (MOIs), may be disclosed from this system as follows:

- (a) To other witnesses when necessary in order to obtain information to further the investigation of the OSC;
- (b) To an actual or potential party or his attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining, or informal discovery proceedings;
- (c) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;
- (d) In the event that a record in this system, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, or tribal law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law;
- (e) In a proceeding before a court or adjudicative body before which the Department of Justice is authorized to appear when (a) the Department of Justice, or any subdivision thereof, is a party to the litigation, (b) any employee of the Department of Justice in his or her official capacity, or (c) any employee of the Department of Justice in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (d) the United States, where the Department of Justice determines that the litigation is likely to affect it or any of its subdivisions, is a party to the litigation or has an interest in litigation and such records are determined by the Department of Justice to be relevant to the litigation.

be arguably relevant to the litigation;

(f) To the news media and the public pursuant to 28 CFR 50.2 (Department of Justice regulations setting forth guidelines for disclosure of information to the media) unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(g) To the General Services Administration and National Archives and Records Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2096; and

(h) To contractors, student interns, or other employees of the OSC to the extent necessary to enable them to perform their assigned duties.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, retaining and disposing of records in the system:

Storage:

All information on this system is stored on a dedicated network server in electronic form. Material is recorded and stored on other data processing storage forms.

Retrievability:

Records are retrieved by names or case numbers or other key word or search term.

Safeguards:

Information in this system is safeguarded in accordance with applicable rules and policies.

including the Department's automated systems security and access policies. All information in the system is password protected and requires access to the OSC's secure internal network. All records and technical equipment are maintained in a central office with restricted access. The facility is secured by the Federal Protective Service.

Retention and disposal:

Records of the investigation shall be transferred to the National Archives at the conclusion of the Special Counsel's work. Administrative and support records shall be disposed of in accordance with General Records Schedules issued by the National Archives and Records Administration (NARA). Standard Form 115, Request for Records Disposition Authority, pending NARA approval.

System manager(s) and address:

John J. Sardar, Assistant Special Counsel, 200 N. Broadway, 15th Floor, St. Louis, Missouri 63102.

Notification procedure:

Address inquiries to System Manager named above.

Record access procedure:

Requests for access must be in writing and should be addressed to the System Manager named above. The envelope and letter should be clearly marked "Privacy Act Access Request." Include in the request the general subject matter of that document(s), and provide your full name and a certification of identity and a return address for response purposes. Information may be exempt from access provisions as described in the section entitled "Systems Exempted from Certain Provisions of the Act." An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should di

their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information may be exempt from contesting record procedures as described in the section entitled "Systems Exempted from Certain Provisions of the Act." An individual who is the subject of a record in this system may amend those records that are exempt. A determination whether a record may be amended will be made at the time a request is received.

Record source categories:

Sources of information contained in this system include but are not limited to documents produced by other federal agencies in response to requests from this office; investigative reports; other non-Department of Justice forensic reports; statements of individuals who have information or knowledge surrounding the events occurring in Waco, Texas on April 1993; verbatim transcripts of deposition and court proceedings including grand jury testimony; public reports; memoranda and reports from court and other agencies; and the work product of the Office of Special Counsel attorneys, investigators, and staff.

Systems exempted from certain provisions of the act:

The Privacy Act authorizes an agency to promulgate rules to exempt any system of records (or part of a system of records) from certain Privacy Act requirements if the system of records is maintained by an agency which performs as its principal function any activity pertaining to the enforcement of criminal laws (5 U.S.C. 552a(j)), or is investigatory material compiled for law enforcement purposes (5 U.S.C. 552a(k)).

The Attorney General has exempted this system from the following Privacy Act requirements: subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j) and (k).

[\[TOP\]](#)

Tax Division

JUSTICE/TAX-001

System Name:

Criminal Tax Case Files, Special Project Files, Docket Cards, and Associated Records.

Security Classification:

Not classified.

System Location:

U.S. Department of Justice, Tax Division, 950 Pennsylvania Avenue, NW., Washington, 20530.

Categories of Individuals Covered by the System:

Persons referred to in potential or actual criminal tax cases or investigations and related matters of concern to the Tax Division under the Internal Revenue laws and related statutes. Since some information about the progress of employees working on the case is retrieved for management purposes, they are also covered by this system.

Categories Of Records In The System:

The system consists of an index, by individual name, of all criminal tax cases and related matters assigned, referred, or of interest to the Tax Division. The records in this system include case files, court records, tax returns, tax return information and documents which contain return information, inter-agency correspondence, intra-agency memoranda, indictments information, search warrants, search warrant affidavits, wiretap authorizations, immunity requests, grand jury information, criminal enforcement and civil investigatory information reports, docket cards, and associated records. For pre-1977 cases or related matters, summary information—names of principals or related parties, case file or management numbers, type, case weight, attorney assigned, court numbers, defense counsel and associated information—is maintained on docket cards. For cases 1977 onwards, information is maintained in an automated case management system. This automated system also permits Tax Division personnel to record information about the case on a comment field. A timekeeping function for attorneys, paralegals, and other Division employees involved in litigation is a part of the automated case management system. Records are maintained for the purpose of prosecuting (including investigations leading to prosecutions) or otherwise resolving criminal cases or matters under the jurisdiction of the Tax Division.

Authority for Maintenance of the System:

This system is established and maintained pursuant to 5 U.S.C. 301, 44 U.S.C. 3101, and 28 U.S.C. 533, and 28 CFR 0.70 and 0.71.

Purposes:

Information is maintained in docket cards and in electronic format on each Tax Division (Division) criminal case and related matter to identify and assign mail to the proper office in the Division and the attorneys therein assigned to the case; to relate incoming material to an existing case; to establish a file and case management numbers; and to provide a central repository of cases within the Division and to facilitate the flow of legal work in the Division. The Division's automated case management system enhances these uses and enables data manager specialists, managers, and Division personnel to locate information about the status of pending or terminated criminal matters and litigation; to identify assigned staff; to track the status of litigation; to prepare reports including budget requests; and to track the number of hours Division personnel worked on various matters.

Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses:

Tax returns and return information may be disclosed only as provided in 26 U.S.C. 6103. Grand jury information may be disclosed only as provided by Rule 6(e) of the Federal Rules of Criminal Procedure.

Other records relating to a case or matter maintained in this system of records may be disseminated as a routine use, as follows:

- (1) Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, state, local, foreign, or tribal, law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.
- (2) In an appropriate proceeding before a court, or administrative or adjudicative body, where the Department of Justice determines that the records are arguably relevant to the proceeding.

or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(3) To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings.

(4) To appropriate officials and employees of a Federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit.

(5) To Federal, state, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

(6) To the National Archives and Records Administration (NARA) for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(7) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(8) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

(9) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

(10) The Department of Justice may disclose relevant and necessary information to a foreign employee of the Department for purposes of: responding to an official inquiry by a Federal, state, or local government entity or professional licensing authority, in accordance with

applicable Department regulations; or facilitating communications with a former employee may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding matter within that person's former area of responsibility.

(11) Information relating to health care fraud may be disclosed to private health plans, associations of private health plans, and health insurers, or associations of health insurers for the following purposes: To promote the coordination of efforts to prevent, detect, investigate and prosecute health care fraud; to assist efforts by victims of health care fraud to obtain restitution; to enable private health plans to participate in local, regional, and national health care fraud task force activities; and to assist tribunals having jurisdiction over claims against private health plans.

(12) In the course of investigating the potential or actual violation of any law whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing for such violation, a record may be disseminated to a Federal, state, local, or foreign agency, or to an individual or organization, if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, trial or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant.

(13) To the referring agency to notify such agency of the status of the case or matter or decision or determination that has been made.

(14) In any health care-related civil or criminal case, investigation, or matter, information indicating patient harm, neglect, or abuse, or poor or inadequate quality of care, at a health care facility or by a health care provider, may be disclosed as a routine use to any federal, state, local, tribal, foreign, joint, international or private entity that is responsible for regulating, licensing, registering, or accrediting any health care provider or health care facility, or enforcing any health care-related laws or regulations. Further, information indicating an ongoing investigation by a health care provider or at a health care facility may be disclosed to the appropriate health plan. Additionally, unless otherwise prohibited by applicable law, information indicating patient harm, neglect, abuse or poor or inadequate quality of care may be disclosed to the affected patient or the patient's representative or guardian at the discretion of and in the manner determined by the agency in possession of the information.

(15) To representatives of the Internal Revenue Service who are conducting tax records

safeguard reviews pursuant to 26 U.S.C. 6103(p)(4).

(16) To the United States Department of State, to the extent necessary to assist in apprehending and/or returning a fugitive to a jurisdiction which seeks the fugitive's return.

Disclosure to Consumer Reporting Agencies:

Only as stated in the above routine uses.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing Records in the System:

Storage:

Unless otherwise noted herein, all information is recorded on paper material and on document cards. Paper materials are stored within file jackets and metal file cabinets; docket card within boxes or card drawers. Summary information, as described above, is maintained in electronic format and stored on data processing-type storage medium or on magnetic tape.

Retrievability:

Information is retrieved primarily by name of person, case or file numbers, employee name or employee number, or court district.

Safeguards:

Information is safeguarded in accordance with 26 U.S.C. 6103(p) and the Tax Division is subject to periodic inspections by the Internal Revenue Service to ensure that adequate safeguards which satisfy the requirements of that section are in place. Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including Department's automated systems security and access policies. The required use of password protection identification features and other system protection methods also restrict access. Access is limited to those officers and employees of the agency who have an official need for access in order to perform their duties. Buildings in which the records are located are under the protection of a security guard, and access to premises is by official identification. The various sections of the Tax Division have locked entry doors which may only be entered with an encrypted card key. Records are stored in spaces and filing cabinets which are locked outside normal business hours.

hours. Training is provided for new Division personnel regarding the need for confidential records, particularly tax returns and return information. A password is required to access automated case management system and passwords are changed every 90 days.

Retention and Disposal:

Tax records not retained are returned to the Internal Revenue Service. Records in close are sent to the Federal Records Center where they are destroyed after fifteen (15) years they are determined to have historical significance under the NARA criteria. Records having historical significance are retained permanently. Summary information in electronic form retained permanently. Closed records designated permanent are retired at the Records where they will remain until the statutory access restrictions of 26 U.S.C. 6103 are resolved.

System Manager(s) and Address:

Assistant Attorney General; Tax Division; U.S. Department of Justice; 950 Pennsylvania Avenue, NW., Washington, DC 20530.

Notification Procedure:

An inquiry concerning this system should be directed to the System Manager listed above.

Record Access Procedures:

Major portions of this system are exempt from disclosure and contest by 5 U.S.C. 552a(the extent that this system of records is not subject to exemption, it is subject to access contest. A determination as to the applicability of an exemption as to a specific record is made at the time a request for access is received. A request for access to a record contained in this system must be made in writing, with the envelope and the letter clearly marked 'Privacy Access Request.' Include in the request the System name, the name of the individual in the individual's birth date and place, or any other identifying number which may be of assistance in locating the record, the name of the case or matter involved, if known, the of the judicial district involved, if known, and any other information which may be of assistance in locating the record. You will also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above. You must sign the request; and, to verify it, the signature must be notarized or submitted under 28 U.S.C. law that permits statements to be made under penalty of perjury and dated as a substituted

notarization. You may submit any other identifying data you wish to furnish to assist in a proper search of the system.

Contesting Record Procedures:

A major part of the information maintained in this system is exempt from this requirement 5 U.S.C. 552a(j)(2). Title 28 U.S.C. 7852(e) prohibits Privacy Act amendment of tax records. Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record Source Categories:

Internal Revenue Service, Department offices and employees, and other Federal, state, and foreign law enforcement and non-law enforcement agencies, private persons, witnesses, and informants.

Exemptions Claimed for the System:

The Attorney General has exempted this system from subsection (c)(3), (c)(4), (d)(1), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register* and are codified at 28 CFR 16.93(a) and (b).

[\[TOP\]](#)

JUSTICE/TAX-002

System Name:

Tax Division Civil Tax Case Files, Docket Cards, and Associated Records.

Security Classification:

Not classified.

System Location:

U.S. Department of Justice; Tax Division; 950 Pennsylvania Avenue, NW., Washington, 20530.

Categories of Individuals Covered by the System:

Persons referred to in potential or actual civil tax cases and related matters under the jurisdiction or of concern to the Tax Division under Internal Revenue laws and related statutes. Since some information about the progress of employees working on the case is retrieved for management purposes, they are also covered by this system.

Categories of Records in the System:

Records in this system pertain to a broad variety of litigation under the jurisdiction of the Division. They include case files which were created or received by the Tax Division in connection with a particular case. These case files contain all pleadings, motions, briefs, transcripts and exhibits, all other papers filed with a court or issued by the Court, correspondence relating to the case, tax returns, tax return information, and documents containing tax return information, inter-agency memoranda, intra-agency memoranda, assignment sheets, investigative reports and associated records. For pre-1977 cases, summary information is maintained on docket cards on which is recorded the names of principals or related parties, case file or management numbers, case type, case weight, attorney assigned, court number, opposing counsel and associated information. For cases beginning in 1977, information is maintained in an automated case management system. This automated system also permits Tax Division personnel to record information about the case on a comment field. Also permitted by the automated case management system is a timekeeping function for attorneys, paralegals and other Tax Division employees involved in litigation.

Authority for Maintenance of the System:

This system is established and maintained pursuant to 5 U.S.C. 301, 44 U.S.C. 3101, a CFR 0.70 and 0.71.

Purposes:

Information is maintained in docket cards and in electronic format on each Tax Division

(Division) civil case: (a) To identify and assign mail to the proper office within the Division; the attorneys therein assigned to the case; (b) to relate incoming material to an existing case; (c) to establish a file and case management numbers; and (d) to provide a central index of cases within the Division and to facilitate the flow of legal work in the Division. The Division's automated case management system enhances these uses and enables data manager specialists, managers, and Division personnel: (a) To locate information about the status of pending or terminated civil matters and litigation; (b) to identify assigned staff; (c) to track the status of litigation; (d) to prepare reports including budget requests; and (e) to track the number of hours Division personnel worked on various matters.

Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses:

Tax returns and return information may be disclosed only as provided in 26 U.S.C. 6103.

Other records related to a case or matter maintained in this system of records may be disseminated as follows:

(1) Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, state, local, foreign, or tribal, law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.

(2) In an appropriate proceeding before a court, or administrative or adjudicative body, where the Department of Justice determines that the records are arguably relevant to the proceeding or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(3) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement or in informal discovery proceedings.

(4) To appropriate officials and employees of a Federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance

grant or benefit.

(5) To Federal, state, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

(6) To the National Archives and Records Administration (NARA) for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(7) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that the release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(8) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

(9) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.

(10) The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee if necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(11) Information relating to health care fraud may be disclosed to private health plans, coalitions of private health plans, and health insurers, or associations of health insurers, for the following purposes: To promote the coordination of efforts to prevent, detect, investigate, and prosecute health care fraud; to assist efforts by victims of health care fraud to obtain restitution; to enable private health plans to participate in local, regional, and national health care fraud task force activities; and to assist tribunals having jurisdiction over claims against

private health plans.

(12) In the course of investigating the potential or actual violation of any law whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation of a trial or hearing for such violation, a record may be disseminated to a Federal, state, local, or foreign agency, or to an individual or organization if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, trial or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant.

(13) A record relating to a case or matter that has been referred to the Tax Division may be disseminated to the referring agency to notify such agency of the status of the case or matter or of any decision or determination that has been made.

(14) In any health care-related civil or criminal case, investigation, or matter, information indicating patient harm, neglect, or abuse, or poor or inadequate quality of care, at a health care facility or by a health care provider, may be disclosed as a routine use to any Federal, state, local, tribal, foreign, international or private entity that is responsible for regulating, licensing, registering, or accrediting any health care provider or health care facility, or enforcing any health care-related laws or regulations. Further, information indicating an ongoing problem by a health care provider or at a health care facility may be disclosed to the appropriate health plan. Additionally, unless otherwise prohibited by applicable law, information indicating harm, neglect, abuse or poor or inadequate quality of care may be disclosed to the affected patient or the patient's representative or guardian at the discretion of and in the manner determined by the agency in possession of the information.

(15) To representatives of the Internal Revenue Service (IRS) who are conducting tax record safeguard reviews pursuant to 26 U.S.C. 6103(p)(4).

(16) To the United States Department of State, to the extent necessary to assist in apprehending and/or returning a fugitive to a jurisdiction which seeks the fugitive's return.

(17) In the case of records relating to an individual who owes an overdue debt to the United States to: (a) A Federal agency which employs the individual to enable the employing agency to offset the individual's salary; (b) a Federal, state, local or foreign agency, an organization including a consumer reporting agency, or individual to elicit information to assist the Department in the collection of the overdue debt; (c) a collection agency or private counsel to enable

to collect the overdue debt; and/or (d) the IRS to enable that agency to offset the individual's tax refund.

Disclosure to Consumer Reporting Agencies:

Only as stated in above routine uses.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing Records in the System:

Storage:

Unless otherwise noted herein, all information is recorded on paper material. Paper materials are stored within file jackets and metal file cabinets; docket cards, within boxes or card drawers. Summary information, as described above, is maintained in electronic format and is stored on data processing-type storage medium or on magnetic tape and docket cards.

Retrievability:

Information is retrieved primarily by name of person, case or file numbers, employee name, employee number, or court district.

Safeguards:

Information is safeguarded in accordance with 26 U.S.C. 6103(p) and the Tax Division is subject to periodic inspections by the IRS to ensure that adequate safeguards which satisfy the requirements of that section are in place. Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including the Department's automated systems security and access policies. The required use of password protection identification features and other system protection methods also restrict access. Access is limited to tax officers and employees of the agency who have an official need for access in order to perform their duties. Buildings in which the records are located are under security guard, and access to premises is by official identification. The various sections in the Division have locked entrance doors which may only be entered with an encrypted card key. Records are stored in space and filing cabinets which are locked outside normal business hours. Training is provided to new Division personnel regarding the need for confidentiality of records, particularly tax and return information. A password is required to access the automated case management system.

system and passwords are changed every 90 days.

Retention and Disposal:

Tax records not retained are sent to the Internal Revenue Service. Records in closed file sent to the Federal Records Center where they are destroyed after fifteen (15) years unless they are determined to have historical significance under the NARA criteria. Records of historical significance are retained permanently. Summary information in electronic form retained permanently. Closed records designated permanent are retired at the Records where they will remain until the statutory access restrictions of 26 U.S.C. 6103 are resolved.

System Manager(s) and Address:

Assistant Attorney General, Tax Division, U.S. Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530.

Notification Procedure:

An inquiry concerning this system should be directed to the System Manager listed above.

Record Access Procedures:

To the extent that this system of records is not subject to exemption, it is subject to access contest. A determination as to the applicability of an exemption to a specific record must be made at the time a request for access is received. A request for access to a record contained in this system must be made in writing, with the envelope and the letter clearly marked 'Privacy Access Request'. Include in the request the System name, the name of the individual in the individual's birth date and place, or any other identifying number which may be of assistance in locating the record, the name of the case or matter involved, if known, the name of the judicial district involved, if known, and any other information which may be of assistance in locating the record. You will also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above. You must sign the request; and, to verify it, the signature must be notarized or submitted under 28 U.S.C. 1792, a law that permits statements to be made under penalty of perjury and dated as a substitute for notarization. You may submit any other identifying data you wish to furnish to assist in making a proper search of the system.

Contesting Record Procedures:

A major part of the information maintained in this system is exempt from this requirement 5 U.S.C. 552a(k)(2). Title 28 U.S.C. 7852(e) prohibits Privacy Act amendment of tax records. Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record Source Categories:

Internal Revenue Service, Department offices and employees, and other Federal, state, and foreign law enforcement and non-law enforcement agencies, private persons, witnesses, and informants.

Exemptions Claimed for the System:

The Attorney General has exempted this system from subsections (c)(3), (d)(1), (d)(2), (d)(4), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and have been published in the *Federal Register* and codified at 28 CFR 16.93 (c) and (d).

[\[TOP\]](#)

JUSTICE/TAX-003

Security Classification:

Not classified.

System Name:

Files of Applications for Attorney and Non-Attorney Positions with the Tax Division.

System Location:

U.S. Department of Justice; Tax Division; 950 Pennsylvania Avenue, NW., Washington, 20530.

Categories of Individuals Covered by the System:

Applicants who have applied for a position as an attorney or for non-attorney positions v Tax Division.

Categories of Records in the System:

The records in this system include resumes, employment applications, referral correspondence, grade transcripts, letters of recommendation, interview notes, internal memoranda and evaluations, information received from references and individuals contacted in connection with the application, and related personnel forms and correspondence. Some information is maintained in electronic format. Summary information (names of applicants, social security numbers, dates documents received, type of documents received, where interviewed, personal data, dispositions, and type of response sent) is maintained in an electronic database.

Authority for Maintenance of the System:

This system is established and maintained pursuant to 5 U.S.C. 301, 44 U.S.C. 3101, a CFR 0.70 and 0.71.

Purpose:

This system is used by employees and officials of the Division and the Justice Department making employment decisions including making information known to references supplied by applicant and other persons contacted to verify information supplied or to obtain additional information.

Routine Uses of Records Maintained in the System, Including Categories of Users and Purposes of Such Uses:

Records related to a case or matter maintained in this system of records may be disseminated as follows:

- (1) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit.
- (2) To the National Archives and Records Administration (NARA) for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.
- (3) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.
- (4) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
- (5) Where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, state, local, foreign, or tribal, law enforcement authority or other appropriate agency charged with the responsibility of investigating or prosecuting such a violation or enforcing or implementing such law.
- (6) To Federal, state, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.
- (7) In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
- (8) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

(9) The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: Responding to an official inquiry by a Federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee, if necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(10) Information may be disclosed to the Office of Personnel Management which conducts audits of these records.

Disclosure to Consumer Reporting Agencies:

Not applicable.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing Records in the System:

Storage:

Unless otherwise noted herein, all information is recorded on paper material. Paper materials are stored within file jackets and metal file cabinets. Summary information, as described, is maintained in electronic format and stored on data processing-type storage medium such as magnetic tape.

Retrievability:

Information is retrieved by using the name of the applicant.

Safeguards:

Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including the Department's automated systems security and access policies. The required use of password protection identification features and other system protection methods also restrict access. Access is limited to those officers and employees of the agency who have an official need for access in order to perform their duties. Buildings in which

records are located are under security guard, and access to premises is by official identification. The Personnel Office in the Division is in a space which has locked key er doors which may only be entered with an encrypted card key. A password is required to an electronic database and passwords are changed every 90 days.

Retention and Disposal:

Information in the applicant files is retained until after a decision is made as to the empl of the applicant, usually for one year and, for some files, up to two years after the decis

Summary information in electronic format is retained permanently. Closed records desig permanent are retired at the Records Center, where they will remain until the statutory r restrictions of 26 U.S.C. 6103 are resolved.

System Manager(s) and Address:

Assistant Attorney General; Tax Division; U.S. Department of Justice; 950 Pennsylvania Avenue, NW., Washington, DC 20530.

Notification Procedure:

An inquiry concerning this system should be directed to the System Manager listed abo

Record Access Procedures:

A request for access to a record contained in this system must be made in writing, with envelope and the letter clearly marked 'Privacy Access Request'. Include in the request name of the individual involved, the individual's birth date and place, or any other identi number which may be of assistance in locating the record, as well as the position applic The requester will also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above. Some information may be exempt from access provisions as described in the section entitled "Exemptions Claimed System." A determination whether a record may be accessed will be made at the time a request is received.

Contesting Record Procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely which information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information may be exempt from contesting records, records procedures, or both, as described in the section entitled "Exemptions Claimed for the System." A determination whether a record, a records procedure(s), or both, may be contested will be made at the time a request is received.

Record Source Categories:

Generally, sources of information contained in the system are the individual applicants, persons referring or recommending the applicant, and employees and officials of the Department and the Department.

Exemptions Claimed for the System:

The Attorney General is exempting this system from 5 U.S.C. 552a subsections (c)(3) and (d)(1), pursuant to 5 U.S.C. 552a(k)(5). The final rule claiming these exemptions is published today's *Federal Register*.

[\[TOP\]](#)

United States Attorney's Office

JUSTICE/USA-001

System name:

Administrative File.

System location:

Ninety-four United States Attorneys' Office (See appendix identified as JUSTICE/USA-94 Executive Office for United States Attorneys, U.S. Department of Justice, 10th & Constitution Avenue NW, Washington, DC 20530).

Categories of individuals covered by the system:

(a) Office Personnel (present and past); (b) Expert professionals whose services are used by the office; (c) Applicants for office positions; (d) Witnesses in Court proceedings; (e) Prisoners in-Custody; (f) Defendants; (g) Debtors; (h) Vendors; (i) Citizens making inquiries; (j) Members of local and State Bar Associations.

Categories of records in the system:

(a) Personnel Files (official/unofficial); (b) Applicant Files; (c) Employee Record cards (SF-50); (d) Office Rosters; (e) Tickler File System for Promotions; (f) Personnel Address and Telephone Number Lists; (g) Sign In/Out Sheets; (h) Time and Attendance Records (OASD-1012); (i) Wage Earnings Statement (DOJ-296); (j) Travel Authorizations and Vouchers (OBD-SF-1012); (k) Advice of Obligations incurred (DJ-60); (l) Telephone Records and Logs; (m) Fiscal Vouchers; (n) Witness Records (LAA-3); (o) Lists of Records at Federal Records Centers; (p) In-House Statistical Reports; (q) Internal Meetings Records; (r) Equal Employment Opportunity (EEO) Records; (s) Employees: Organizations and Unions Records; (t) Federal Woman's Program Records; (u) Address and Telephone Indexes; (v) Lists of State and Bar Members; (w) Lists of Expert Professionals; (x) Requests for Expert Witnesses; (y) Telephone Files; (z) Correspondence Files; and (aa) Assistant United States Attorneys' Inventory.

Authority for maintenance of the system:

These systems are established and maintained pursuant to 5 U.S.C. 301 and 44 U.S.C. 3101.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of the system of records as follows:

(a) In any case in which there is an indication of a violation or potential violation of law or regulation, criminal, civil, or regulatory in nature, the record in question may be disseminated to the appropriate federal, state, local, or foreign agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law or civil remedy;

(b) In the course of investigating the potential or actual violation of any law, criminal, civil,

regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing for such violation, a record may be disseminated to a federal, state, local, or foreign agency, or to an individual or organization, if there is reason to believe that such agency or individual or organization possesses information relating to the investigation, trial or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant;

(c) A record relating to a case or matter may be disseminated in an appropriate federal, state, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive or procedural law or practice;

(d) A record relating to a case or matter may be disseminated to a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing;

(e) A record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion on such matters as settlement of a case or matter, plea bargaining, or informal discovery proceedings;

(f) A record relating to a case or matter that has been referred by an agency for investigation, prosecution, or enforcement, or that involves a case or matter within the jurisdiction of a federal agency, may be disseminated to such agency to notify the agency of the status of the case or matter or of any decision or determination that has been made, or to make such other inquiries and reports as are necessary during the processing of the case or matter;

(g) A record relating to a person held in custody pending or during arraignment, trial, sentencing, or extradition proceedings, or after conviction or after extradition proceedings, may be disseminated to a federal, state, local, or foreign prison, probation, parole, or pardon authority or to any other agency or individual concerned with the maintenance, transportation, or care of such a person;

(h) A record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States or to a foreign executive agreement;

(i) A record may be disseminated to a federal, state, local, foreign, or international law

enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency;

(j) A record may be disseminated to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the request for an investigation of an employee, the letting of a contract, or the issuance of a license or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter;

(k) A record may be disseminated to the public, news media, trade associations, or other groups, when the purpose of the dissemination is educational or informational, such as descriptions of crime trends or distinctive or unique modus operandi, provided that the record does not contain any information identifiable to a specific individual other than such modus operandi;

(l) A record may be disseminated to a foreign country, through the United States Department of State or directly to the representative of such country, to the extent necessary to assist the country in apprehending and/or returning a fugitive to a jurisdiction which seeks his return;

(m) A record that contains classified national security information and material may be disseminated to persons who are engaged in historical research projects, or who have previously occupied policymaking positions to which they were appointed by the President in accordance with the provisions codified in 28 CFR 17.60; and

(n) A record may be accessed by volunteer student workers and students working under a college work-study program, as is necessary to enable them to perform their function.

Release of information to the news media:

Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice, unless it is determined that release of the specific information in the context of a particular request would constitute an unwarranted invasion of personal privacy.

Release of information to Member of Congress:

Information contained in systems of records maintained by the Department of Justice, in

otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration:

A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

All information except that specified in this paragraph, is recorded on basic paper/card material, and stored within manila file folders, within metal file cabinets, electric file/cabinet retrievers or safes. Some material is recorded and stored on magnetic tape, card or other electronic processing type storage matter for reproduction later into conventional formats.

Retrievability:

Information is retrieved primarily by name of person, case number, complaint number or docket number. Information within this system of records may be accessed by various U.S. Attorney's offices and the Executive Office for United States Attorneys by means of cathode ray tube terminals (CRT's).

Safeguards:

Information in the system is stored in file cabinets in the United States Attorney's offices. Materials are located in locked file drawers and safes, and others in unlocked file drawers. Offices are locked during non-working hours and are secured by either Federal Protective Service, United States Postal Service, or private building guards. Information that is retrieved by CRT's within various U.S. Attorneys' offices and the Executive Office for United States Attorneys requires user identification numbers which are issued to authorized employees of the Department of Justice.

Retention and disposal:

Records are maintained and disposed of in accordance with Department of Justice retention plans.

System manager(s) and address:

System Manager for the system in each office is the Administrative Officer/Assistant, for U.S. Attorney for each district (See appendix identified as JUSTICE/USA-999).

Notification procedure:

Address inquiries to the System Manager for the judicial district in which the case or matter is pending (See appendix identified as JUSTICE/USA-999).

Record access procedures:

A request for access to a record from this system shall be made in writing with the envelope and the letter clearly marked "Privacy Access Request." Include in the request the name of the individual involved, his birth date and place, or any other identifying number or information which may be of assistance in locating the record and the name of the case or matter involved, if known. The requester will also provide a return address for transmitting the information. Access requests will be directed to the System Manager (See appendix identified as JUSTICE/USA-999).

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should di

their request to the System manager (See appendix identified as JUSTICE/USA-999) state clearly and concisely what information is being contested, the reasons for contesting it, proposed amendment to the information sought.

Record source categories:

Sources of information contained in this system include, but are limited to, investigative of federal, state and local law enforcement agencies, client agencies of the Department of Justice; other non-Department of Justice investigative agencies; forensic reports; statements of witnesses and parties, data, memoranda and reports from the Courts and agencies thereof and the work product of Assistant United States Attorneys, Department of Justice attorneys and administrative staff of the divisions, offices and bureaus, work product of secretarial and administrative staff within the U.S. Attorneys office and the Executive Office for U.S. Attorneys; information from general public referral sources or as provided by members of the public who participate or observe in pending cases or matters, or commercial establishments which provide goods or services, publications and reports from the Department's other offices, division bureaus and internal U.S. Attorney work product.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/USA-002

System name:

A U.S.A. Applicant Files.

System location:

Executive Office for United States Attorneys, U.S. Department of Justice, 10th & Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

Applicants tentatively selected (by nomination of a U.S. Attorney) for the position of Assistant United States Attorney.

U.S. Attorney.

Categories of records in the system:

The system includes the applicants name, status of Bar membership and dates of receipt of status and final determination on the appointment of the applicant. The system is arranged chronologically by date of receipt of file and applicants name.

Authority for maintenance of the system:

These records are kept for administrative convenience pursuant to 5 U.S.C. 301 and 44 U.S.C. 3101.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

All uses are internal within the Department.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress. Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes

responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

The material is stored within manila file folders, within metal file cabinets.

Retrievability:

The system is indexed by name, arranged alphabetically.

Safeguards:

The correspondence is maintained in a room which is occupied by office personnel during the day and locked at night.

Retention and disposal:

Records are maintained and disposed of in accordance with Department retention plans.

System manager(s) and address:

Director, Executive Office of United States Attorneys, U.S. Department of Justice, 10th & Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Same as the above.

Record access procedures:

A request for access to a record from this system shall be made in writing, with the envelope

and the letter clearly marked "Privacy Access Request." Include in the request the name, address as included in the original letter, together with the current address if different, the date of the letter and to whom it was addressed. Requests should be directed to the System Manager listed above.

Contesting record procedures:

Any requests for correction should also be directed to the System Manager and should include the exact correction required.

Record source categories:

Sources of information in this system are the actual letter received, the response and any information transmitted and enclosures.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/USA-003

System name:

Citizen Complaint Files.

System location:

U.S. Attorney's Office, Judiciary Center Bldg., 555 4th St. NW, Washington, DC 20001; Executive Office for United States Attorneys, U.S. Department of Justice, 10th & Constitution Avenue, NW., Washington, DC 20530.

Categories of individuals covered by the system:

The individuals on whom records are maintained in this system may be broadly classified into four categories. (1) Those individuals who have been charged with Federal and D.C. Crimes.

violations; (2) those individuals who are currently under investigation for violations of Fe and D.C. Code; (3) those individuals about whom complaints have been made on upon investigations were conducted, but no prosecution was initiated; and (4) complainants.

Categories of records in the system:

A file may consist of a single sheet of paper describing briefly the nature of a complaint disposition or it may consist of a more comprehensive file containing the results of a hearing depending on the complexity or seriousness of the complaint. If the complaint results in criminal charges being preferred, the contents of the file are transferred to the appropriate criminal file system.

Authority for maintenance of the system:

5 U.S.C. 301, 28 U.S.C. 547, 23 D.C. Code 101(c).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of a record as follows:

(1) In any case in which there is an indication of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, the record in question may be disseminated to the appropriate agency, federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcement or implementing laws;

(2) In the course of investigating the potential or actual violation of any law, whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation of a trial or hearing for such violation, a record may be disseminated to a federal, state, local, or foreign agency, or to an individual, if there is reason to believe that such agency or individual possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or informant;

(3) Records or extracts thereof relating to case matters or matters may be disseminated to

defendant or his attorney or to the appropriate federal, state, local or foreign court or grand jury in accordance with established constitutional, substantive, or procedural law or practice

(4) A record relating to a case or matter may be disseminated to a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing;

(5) A record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion on such matters as settlement of a case or matter, plea bargaining, or informal discovery proceedings;

(6) A record relating to a case or matter that has been referred for investigation may be disseminated to the referring agency to notify such agency of the status of the case or matter or of any decision or determination that has been made;

(7) A record relating to a person held in custody, arrest, trial or sentence, or after conviction, may be disseminated to a federal, state, local, or foreign prison, probation, parole, bail or pardon authority, or to any agency or individual, concerned with the custody, maintenance, transportation, or release of such person;

(8) A record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States;

(9) A record may be disseminated to a federal, state, local, or foreign law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency;

(10) A record may be disseminated to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter;

(11) A record may be accessed by volunteer student workers and students working under a college work-study program, as is necessary to enable them to perform their function.

(12) Release of information to the news media: Information permitted to be released to the

news media and the public pursuant to 28 CFR 50.2 may be made available from system records maintained by the Department of Justice unless it is determined that release of specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(13) Release of information to Members of Congress. Information contained in systems records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of the individual who is the subject of the record and;

(14) Release of information to the National Archives and Records Administration (NARA) and the General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Citizen complaint files are maintained in one of two ways; either on a single sheet which is a record of the complaint and disposition thereof or in complaints which result in further proceedings, a file folder would be established. Some material is recorded and stored on magnetic tape, card or other data processing type storage medium for reproduction later in conventional formats and for management information purposes.

Retrievability:

Information is retrieved either by the name of a complainant, the name of a person about whom a complaint is registered or by a complaint number. If further proceedings are conducted with respect to a citizen's complaint and the complaint materializes into a criminal action, the file folder will become part of the criminal files and then is retrievable in the same manner as a criminal file is retrieved. Information may be accessed by means of cathode-ray tube terminals (CRT'S).

Safeguards:

Information contained in the system is unclassified. It is safeguarded and protected by being maintained in files at the Citizens Complaint Center, and the Legal Services section of the Executive Office for United States Attorneys, which is manned at all times when it is open and at other times is locked. More sensitive files that materialize into hearings or require further action by the Misdemeanor Trial Section of the Superior Court Division, or the Executive Office for United States Attorneys, are maintained by the Chief of the Misdemeanor Trial Section in office in Building B of the Superior Court, or the Assistant Director for Legal Services, Executive Office for United States Attorneys in his safe. Information that is retrievable by CRT's with various U.S. Attorneys' offices and the Executive Office for United States Attorneys requires identification numbers which are issued to authorized employees of the Department of Justice.

Retention and disposal:

Files are retained and disposed of in accordance with Title 3, U.S. Attorney's Manual.

System manager(s) and address:

Chief, Misdemeanor Trial Section, U.S Attorney's Office, Superior Court, Operations, 55 Constitution Avenue, NW, Washington, DC 20001; Director, Executive Office for United States Attorneys, Department of Justice, 10th & Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Address inquiries to the System Manager.

Record access procedures:

The major part of these systems are exempt from this requirement under 5 U.S.C. 552a (k)(1) and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to public access. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record from this system shall be made in writing, with the request in an envelope and the letter clearly marked "Privacy Access Request." Include in the request the general subject matter of the document or its file number. The requestor will also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

The major parts of these systems are exempt from this requirement under 5 U.S.C. 552 (k)(1) and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to contest. A determination as to exemption shall be made at the time a request for contest is received. Individuals desiring to contest or amend information maintained in the system shall direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in this system come primarily from citizens walking into a unit to register complaints. Sources also include but are not limited to investigative reports from federal, state and local law enforcement agencies, forensic reports, statements of witnesses and parties, as well as verbatim transcripts for grand jury proceedings and court proceedings, memoranda and reports from the court and agencies thereof and the work product of Assistant United States Attorneys and legal assistants working on particular cases.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(4)(G) and (H), (e)(5) and (8), (f), (g) and (h) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k)(1) and (2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/USA-005

System name:

Civil Case Files.

System location:

Ninety-four United States Attorneys' Offices (See Appendix identified as Justice/USA-96) Executive Office for United States Attorneys, U.S. Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

(a) Individuals being investigated in anticipation of Civil suits; (b) Individuals involved in suits; (c) Defense Counsel(s); (d) Information sources; (e) Individuals relevant to the development of Civil suits.

Categories of records in the system:

(a) All Civil Case Files (USA-34); (b) Docket Cards (USA-116); (c) Civil Debtor Cards—(USA-117b); (d) Civil Case Activity Card (USA-164); (e) Civil Debtor Activity Card (USA-164); (f) 3 x 5 Index Cards; (g) Caseload Printouts; (h) General Correspondence re: Civil Cases; (i) Reading Files re: Civil Cases; (j) Information Source File; (k) Attorney Assignment sheet; (l) Telephone records; (m) Miscellaneous Investigative files; (n) Lands condemnation files (Appraisal and Negotiator Reports); (o) Tax Case Resource File; (p) Material in Civil File to Criminal cases arising out of Civil Proceedings; (q) Search Warrants; (r) Files unique to District; (s) Civil Miscellaneous Correspondence File.

Authority for maintenance of the system:

These systems are established and maintained pursuant to 5 U.S.C. 301, 28 U.S.C. 541, and 44 U.S.C. 3101.

Purpose(s):

Records are maintained for the purpose of litigating or otherwise resolving civil cases or matters handled by the United States Attorneys or the Executive Office for United States Attorneys.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of the system if the record as follows:

(a) In any case in which there is an indication of a violation or potential violation of law, or a matter that is regulatory in nature, the record in question may be disseminated to the appropriate Federal, State, local or foreign agency charged with the responsibility of investigating, defending

pursuing such violation, civil claim or remedy, or charged with enforcing, defending or implementing such law;

(b) In the course of investigating the potential or actual violation or civil liability of any government action or law, civil, or regulatory in nature or during the course of a trial or hearing or the preparation for a trial or hearing for such civil action, a record may be disseminated to a Federal, State, local, or foreign agency, or to an individual or organization, if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation or civil action trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an agency;

(c) A record relating to a case or matter may be disseminated in an appropriate Federal, State, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practice;

(d) A record relating to a case or matter may be disseminated to a Federal, State, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing;

(e) A record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, or informal discovery proceedings;

(f) A record relating to a case or matter that has been referred by an agency for investigation, civil action, or enforcement, or that involves a case or matter within the jurisdiction of an agency, may be disseminated to such agency to notify the agency of the status of the case or matter or of any decision or determination that has been made, or to make such other inquiries and reports as are necessary during the processing of the case or matter;

(g) A record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States or to an executive agreement;

(h) A record may be disseminated to a Federal, State, local, foreign, or international law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency or to assist in general

matters or cases;

(i) A record may be disseminated to a Federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of security clearance as is required for the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter;

(j) A record may be disseminated to the public, news media, trade associations, or other groups, when the purpose of the dissemination is educational or informational, such as descriptions of types or courses of action or distinctive or unique modus operandi, provided that the record does not contain any information identifiable to a specific individual other than the such modus operandi;

(k) A record may be disseminated to a foreign country, through the United States Department of State or directly to the representative of such country, to the extent necessary to assist such country in general crime prevention, the pursuit of general civil, regulatory or administrative actions or to provide investigative leads to such country, or assist in the location and/or returning of witnesses and other evidence;

(l) A record that contains classified national security information and material may be disseminated to persons who are engaged in historical research projects, or who have previously occupied policy making positions to which they were appointed by the President in accordance with the provisions codified in 28 CFR 17.96;

(m) A record relating to an actual or potential civil or criminal violation of title 17, United States Code, may be disseminated to a person injured by such violation to assist him in the institution or maintenance of a suit brought under such title;

(n) A record may be accessed by volunteer student workers and students working under a college work-study program, as is necessary to enable them to perform their function;

(o) A record, or facts derived therefrom, may be disseminated in a proceeding before a court or an adjudicative body before which the United States Attorney's office or the Executive Office for U.S. Attorneys is authorized to appear when (i) the United States Attorney's office or the Executive Office for U.S. Attorneys, or any subdivision thereof, or (ii) any employee of the

United States Attorney's office or the Executive Office for U.S. Attorneys in his or her official capacity, or (iii). any employee of the United States Attorney's office or the Executive Office for U.S. Attorneys in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (iv). the United States, where the United States Attorney's office or the Executive Office for U.S. Attorneys determines that the litigation is likely to affect it or its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the United States Attorney's office or the Executive Office for U.S. Attorneys to be arguably relevant to the litigation;

(p) A record, or facts derived therefrom, may be disseminated in a proceeding before a judicial or adjudicative body before which the United States Attorney's Office is authorized to appear when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by the United States Attorney's Office to be arguably relevant to the litigation;

(q) In any health care related civil or criminal case, investigation, or matter, information indicating patient harm, neglect, or abuse, or poor or inadequate quality of care, at a health care facility or by a health care provider, may be disclosed as a routine use to any federal, state, local, tribal, foreign, joint, international or private entity that is responsible for regulating, licensing, registering, or accrediting any health care provider or health care facility, or enforcing any health care related laws or regulations. Further, information indicating an ongoing quality of care problem by a health care provider or at a health care facility may be disclosed to the appropriate health plan. Additionally, unless otherwise prohibited by applicable law, information indicating patient harm, abuse or poor or inadequate quality of care may be disclosed to the affected patient or his or her representative or guardian at the discretion of the agency in the manner determined by the agency in possession of the information;

(r) Records relating to an individual who owes an overdue debt to the United States may be disseminated to (1) a Federal agency which employs the individual to enable the employing agency to offset the individual's salary, (2) a Federal, State, local or foreign agency, an organization, including a consumer reporting agency, or individual to elicit information to assist the United States Attorney in the collection of the overdue debt, (3) a collection agency or private counsel to enable them to collect the overdue debt, and (4) the Internal Revenue Service (IRS) to enable that agency to offset the individual's tax refund. Records provided to the IRS may be used in a computer matching program to identify individuals who are eligible for refunds against which such offset for overdue debts would be appropriate;

(s) Information permitted to be released to the news media and the public pursuant to 25 U.S.C. 50.2 may be made available unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(t) Information not otherwise required to be released pursuant to 5 U.S.C. 552, may be released to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of this record;

(u) A record may be disclosed as a routine use to the National Archives and Records Administration in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906; and Notice of disclosure under subsection (b)(12) of the Privacy Act: Records relating to individuals who owe a past-due debt to the United States may be disseminated to consumer reporting agencies to encourage payment of the past-due debt.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information relating to health care fraud may be disclosed to private health plans, or associations of private health plans, and health insurers, or associations of health insurers, for the following purposes: to promote the coordination of efforts to prevent, detect, investigate, and prosecute health care fraud; to assist efforts by victims of health care fraud to obtain restitution; to enable private health plans to participate in local, regional, and national health care fraud task force activities; and to assist tribunals having jurisdiction over claims against private health plans.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system

Storage:

All information, except that specified in this paragraph, is recorded on basic paper/card material, and stored within manila file folders, within metal file cabinets, electric file/card retrievers or safes. Some material is recorded and stored on magnetic tape, card or other processing type storage matter for reproduction later into conventional formats.

Retrievability:

Information is retrieved primarily by name of person, case number, complaint number or docket number. Information within this system of records may be accessed by various U.S. Attorneys' offices, and the Executive Office for United States Attorneys by means of cathode-ray tube terminals (CRT's).

Safeguards:

Information in the system is both confidential and nonconfidential and located in file cabinets at the United States Attorney offices.

Confidential materials are in locked file drawers and safes, and nonconfidential material in unlocked file drawers. Offices are locked during nonworking hours and are secured by U.S. Marshals, Federal Protective Service, United States Postal Service, or private building guards. Information that is retrievable by CRT's within various U.S. Attorney's offices and the Executive Office for United States Attorneys requires user identification numbers which are issued to authorized employees of the Department of Justice.

Retention and disposal:

Records are destroyed ten years after case is closed in accordance with approved retention and disposal schedules.

System manager(s) and address:

System Manager for the system in each office is the Administrative Officer/Assistant, for the U.S. Attorney for each district. (See appendix.)

Notification procedure:

Address inquiries to the System Manager for the judicial district in which the case or matter is pending. (See appendix.)

Record access procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a (j)(2), (k)(1) and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to access. A determination as to whether an exemption applies shall be made at the time a request for access is received. A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." Include in the request the name of the individual involved, his birth date and place, or any other identifying number or information which may be of assistance in locating the record, the name of the case or matter involved, if known. The requestor will also provide his or her notarized signature and a return address for transmitting the information. Access requests shall be directed to the System Manager. (See appendix.)

Contesting record procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a (j)(2), (k)(1) and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to contest. A determination as to whether an exemption applies shall be made at the time a request for contest is received. Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager (see appendix) stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in this system include, but are not limited to, investigative reports of Federal, State, and local law enforcement, civil litigation, regulatory and administrative agencies; client agencies of the Department of Justice; other non-Department of Justice investigative agencies; forensic reports; statements of witnesses and parties; verbatim transcripts of deposition and court proceedings; diaries, memoranda and reports from the agencies and agencies thereof; and the work product of Assistant United States Attorneys, Department of Justice attorneys and staff, and legal assistants working on particular cases.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c) (3) and (4), (d), (e) (2) and (3), (e)(4) (G) and (H), (e) (5) and (8), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k) (1) and (2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c), and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/USA-006

System name:

Consumer Complaints.

System location:

U.S. Attorney's Office, Judiciary Center Bldg., 555 4th St. NW, Washington, DC 20001.

Categories of individuals covered by the system:

The individuals on whom records are maintained in this system may be broadly classified into four categories: (1) Those individuals who have been charged with Federal and D.C. Code violations; (2) Those individuals who are currently under investigation for violations of Federal and D.C. Code; (3) Those individuals upon whom investigations were conducted, but no prosecution was initiated; and (4) Complainants.

Categories of records in the system:

The system contained allegations of consumer fraud by citizens of the District of Columbia Metropolitan area. It includes names, addresses, and the substance of the complaints.

Authority for maintenance of the system:

5 U.S.C. 301.28 U.S.C. 547.23 D.C. Code 101(c).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in the system of records may be disseminated as a routing use of a record as follows:

- (1) In any case in which there is an indication of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, the record in question may be disseminated to the appropriate agency, federal, state, local, or foreign, charged with enforcing or implementing such law;
- (2) In the course of investigating the potential or actual violation of any law, whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation of a trial or hearing for such violation, a record may be disseminated to a federal, state, local, or foreign agency, or to an individual, if there is reason to believe that such agency or individual possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or informant;
- (3) Records or extracts thereof relating to a case or matter may be disseminated to a defendant or his attorney or to the appropriate federal, state, local, or foreign, court or grand jury in accordance with established constitutional, substantive, or procedural law or practice;
- (4) A record relating to a case or matter may be disseminated to a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing;
- (5) A record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion on such matters as settlement of a case or matter, plea bargaining, or informal discovery proceedings;
- (6) A record relating to a case or matter that has been referred for investigation may be disseminated to the referring agency to notify such agency of the status of the case or matter or of any decision or determination that has been made;
- (7) A record relating to a person held pending arraignment, trial or sentence, or after conviction may be disseminated to a federal, state, local or foreign prison, probation parole, bail or release authority, or to any agency or individual concerned with the custody maintenance, transportation, or release of such a person;

(8) A record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty of convention entered into or ratified by the United States;

(9) A record may be disseminated to federal, state, local, or foreign law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency;

(10) A record may be disseminated to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter; and

(11) A record may be accessed by volunteer student workers and students working under a college work-study program, as is necessary to enable them to perform their function.

(12) Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from system records maintained by the Department of Justice unless it is determined that release of specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(13) Release of information to Members of Congress: Information contained in systems or records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information on behalf of the individual who is the subject of the record and;

(14) Release of information to the National Archives and Records Administration (NARA) and the General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional

licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Information relating to health care fraud may be disclosed to private health plans, or associations of private health plans, and health insurers, or associations of health insurers, for the following purposes: to promote the coordination of efforts to prevent, detect, investigate and prosecute health care fraud; to assist efforts by victims of health care fraud to obtain restitution; to enable private health plans to participate in local, regional, and national health care fraud task force activities; and to assist tribunals having jurisdiction over claims against private health plans.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in this system is stored in the Fraud Section of the U.S. Attorney General's Office.

Retrievability:

Information is retrieved via a cross-index by complainant and potential defendant.

Safeguards:

Information contained in this system is unclassified. It is protected in accordance with Departmental rules and is safeguarded in the U.S. Attorney's Office in the Fraud Section.

Retention and disposal:

The records are stored for a period of at least the statute of limitations for the offense charged.

System manager(s) and address:

Chief, Fraud Division, U.S. Attorney's Office, Judiciary Center Bldg., 555 4th Street, NW
Washington, DC 20001.

Notification procedure:

Address inquiries to the System Manager.

Record access procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a (j)(2), (k)(1) and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to access. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." Include with the request the general subject matter of the document or its file number. The requestor shall also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a (j)(2), (k)(1) and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to contest. A determination as to exemption shall be made at the time a request for contest is received. Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

The sources of information contained in this system are complaints referred to the U.S. Attorney's Office by citizens and consumer protection agencies.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(4)(G) and (H), (e)(5) and (8), (f), (g) and (h) of the Privacy Act pursuant to 5 552a (j)(2) and (k)(1) and (2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal R*

[\[TOP\]](#)

JUSTICE/USA-007

System name:

Criminal Case Files.

System location:

Ninety-four United States Attorneys' Offices (See Appendix identified as Justice/USA-99 Executive Office for United States Attorneys, U.S. Department of Justice, 10th and Constitution Avenue NW, Washington, DC 20530; and posted on the internet website of the EOUSA <http://www.usdoj.gov/eousa>.

Categories of individuals covered by the system:

(a) Individuals charged with violations; (b) Individuals being investigated for violations; (c) Defense Counsel(s); (d) Information Sources; (e) Individuals relevant to development of Criminal Cases; (f) Individuals investigated, but prosecution declined; (g) Individuals referred in potential or actual cases and matters of concern to a U.S. Attorney's Office; (h) Individuals placed into the Department's Pretrial Diversion program.

Categories of records in the system:

(a) All case files (USA-33); (b) Docket Cards (USA-115); (c) Criminal Debtor Cards (USA-117a); (d) Criminal Case Activity Card (USA-163); (e) Criminal Debtor Activity Card (USA-164); (f) 3 by 5 Index Cards; (g) Caseload Printouts; (h) Attorney Assignment Sheet; (i) General Correspondence re: Criminal Cases; (j) Reading Files re: Criminal Cases; (k) Grand Jury Proceedings; (l) Miscellaneous Investigative Reports; (m) Information Source Files; (n) Parole Recommendations; (o) Immunity Requests; (p) Witness Protection Files; (q) Wiretap Authorizations; (r) Search Warrants; (s) Telephone Records; (t) Criminal Complaints; (u)

Sealed Indictment Records; (v) Files Unique to a District; (w) Criminal Miscellaneous Correspondence File; (x) Prosecution Declined Reports.

Authority for maintenance of the system:

These systems are established and maintained pursuant to 5 U.S.C. 301, 28 U.S.C. 541, 44 U.S.C. 3101.

Purpose(s):

Records are maintained for the purpose of prosecuting or otherwise resolving criminal matters handled by the United States Attorneys.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of a record as follows:

(a) In any case in which there is an indication of a violation or potential violation of law, criminal, civil, or regulatory in nature, the record in question may be disseminated to the appropriate Federal, state, local, or foreign agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(b) In the course of investigating the potential or actual violations of any law, criminal, civil, or regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing for such violation, a record may be disseminated to a Federal, state, local, or foreign agency, or to an individual or organization, if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant;

(c) A record relating to a case or matter may be disseminated in an appropriate Federal, state, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practice;

(d) A record relating to a case or matter may be disseminated to a Federal, state, or local

administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing;

(e) A record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion on such matters as settlement of a case or matter, plea bargaining, or informal discovery proceedings;

(f) A record relating to a case or matter that has been referred by an agency for investigation, prosecution, or enforcement, or that involves a case or matter within the jurisdiction of an agency, may be disseminated to such agency to notify the agency of the status of the case or matter or of any decision or determination that has been made, or to make such other inquiries and reports as are necessary during the processing of the case or matter;

(g) A record relating to a person held in custody pending or during arraignment, trial, sentencing, or extradition proceedings, or after conviction or after extradition proceedings, may be disseminated to a Federal, state, local, or foreign prison, probation, parole, or pardon authority or to any other agency or individual concerned with the maintenance, transportation, or care of such a person;

(h) A record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States or to an executive agreement;

(i) A record may be disseminated to a Federal, state, local, foreign, or international law enforcement agency to assist in the general crime prevention and detection efforts of that agency or to provide investigative leads to such agency;

(j) A record may be disseminated to a Federal agency, in response to its request, in connection with the hiring or retention of any employee, the issuance of a security clearance, the release of an investigation of an employee, the letting of a contract, or the issuance of a license or other benefit by the requesting agency, to the extent that the information relates to that agency's decision on the matter;

(k) A record may be disseminated to the public, news media, trade associations, or other groups, when the purpose of the dissemination is educational or informational, such as descriptions of crime trends or distinctive or unique modus operandi: Provided that the information

does not contain any information identifiable to a specific individual other than such moi operandi;

(l) A record may be disseminated to a foreign country through the United States Department of State or directly to the representative of such country, to the extent necessary to assist such country in apprehending and/or returning a fugitive to a jurisdiction which seeks his return;

(m) A record that contains classified national security information and material may be disseminated to persons who are engaged in historical research projects, or who have previously occupied policy making positions to which they were appointed by the President in accordance with the provisions codified in 28 CFR 17.96;

(n) A record relating to an actual or potential civil or criminal violation of title 17, United States Code, may be disseminated to a person injured by such violation to assist him in the institution or maintenance of a suit brought under such title;

(o) Information permitted to be released to the news media and the public pursuant to 28 CFR 17.50.2 may be made available unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(p) Information not otherwise required to be released pursuant to 5 U.S.C. 552 may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record;

(q) A record may be disclosed as a routine use to the National Archives and Records Administration in records management inspections conducted under the authority of 44 CFR 2904 and 2906;

(r) A record may be accessed by volunteer student workers and students working under a college work-study program, as is necessary to enable them to perform their function;

(s) A record, or facts derived therefrom, may be disseminated in a proceeding before a court or an adjudicative body before which the United States Attorney's office or the Executive Office for U.S. Attorneys is authorized to appear when i. the United States Attorney's office or the Executive Office for U.S. Attorneys, or any subdivision thereof, or ii. any employee of the

States Attorney's office or the Executive Office for U.S. Attorneys in his or her official capacity or iii. any employee of the United States Attorney's office or the Executive Office for U.S. Attorneys in his or her individual capacity where the Department of Justice has agreed to represent the employee, or iv. the United States, where the United States Attorney's office or the Executive Office for U.S. Attorneys determines that the litigation is likely to affect it or its subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the United States Attorney's office or the Executive Office for U.S. Attorneys to be arguably relevant to the litigation;

(t) A record, or facts derived therefrom, may be disseminated in a proceeding before a court or adjudicative body before which the United States Attorney's office is authorized to appear when the United States, or any agency or subdivision thereof, is a party to litigation or has an interest in litigation and such records are determined by the United States Attorney's office to be arguably relevant to the litigation;

(u) In any health care related civil or criminal case, investigation, or matter, information indicating patient harm, neglect, or abuse, or poor or inadequate quality of care, at a health care facility or by a health care provider, may be disclosed as a routine use to any federal, state, local, tribal, foreign, joint, international or private entity that is responsible for regulating, licensing, registering, or accrediting any health care provider or health care facility, or enforcing any health care related laws or regulations. Further, information indicating an ongoing problem of care by a health care provider or at a health care facility may be disclosed to an appropriate health plan. Additionally, unless otherwise prohibited by applicable law, information indicating patient harm, abuse or poor or inadequate quality of care may be disclosed to the affected patient or his or her representative or guardian at the discretion of the agency in the manner determined by the agency in possession of the information.

(v) Records relating to an individual who owes an overdue debt to the United States may be disseminated to (1) a Federal agency which employs the individual to enable the employer agency to offset the individual's salary, (2) a Federal, State, local or foreign agency, an organization, including a consumer reporting agency, or individual to elicit information to assist the United States Attorney in the collection of the overdue debt, (3) a collection agency or private counsel to enable them to collect the overdue debt, and (4) the Internal Revenue Service (IRS) to enable that agency to offset the individual's tax refund. Records provided to the IRS may be used in a computer matching program to identify individuals who are overpaid refunds against which such offset for overdue debts would be appropriate; and Notice of disclosure under Subsection (b)(12) of the Privacy Act: Records relating to individuals who

a past-due debt to the United States may be disseminated to consumer reporting agency to encourage payment of the past-due debt.

(w) information may be disclosed to complainants and victims to the extent necessary to provide them with information concerning the progress or results of the investigation or arising from the matters of which they complained or were the victim.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

All information except that specified in this paragraph, is recorded on basic paper/card material, and stored within manila file folders, within metal file cabinets, electric file/card retrievers or safes. Some material is recorded and stored on magnetic tape, card or other processing type storage matter for reproduction later into conventional formats.

Retrievability:

Information is retrieved primarily by name of person, case number, complaint number or docket number. Information within this system of records may be accessed by various U.S. Attorney's offices and the Executive Office for United States Attorneys by means of cathode ray tube terminals (CRTs).

Safeguards:

Information in the system is both confidential and non-confidential and located in file cabinets in the United States Attorney offices.

Confidential materials are in locked file drawers and safes, and nonconfidential material in unlocked file drawers. Offices are locked during non-working hours and are secured by Federal Protective Service, United States Postal Service, or private building guards. Information that is retrievable by CRTs within various U.S. Attorney's offices and the Executive Office of United States Attorneys requires user identification numbers which are issued to authorized employees of the Department of Justice.

Retention and disposal:

Case files involving no sentence, or sentences of ten years or less, are destroyed ten years after case is closed. Case files involving sentences of more than ten years are destroyed one year after the date of termination of sentence. Both are in accordance with approved retention and disposal schedules.

System manager(s) and address:

System manager for the system in each office is the Administrative Office/Assistant, for U.S. Attorney for each district (See appendix or EOUSA internet address of <http://www.usdoj.gov/eousa>).

Notification procedure:

Address inquiries to the System Manager for the judicial district in which the case or matter is pending (See appendix or EOUSA internet address of <http://www.usdoj.gov/eousa>).

Record access procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a(j)(2), (k)(1) and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to access. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." Include in the request the name of the individual involved, his birth date and place, or any other identifying number or information which may be of assistance in locating the record and the name of the case or matter involved, if known. The requester will also provide his or her notarized signature and a return address for transmitting the information. Access request

be directed to the System Manager (See appendix).

Contesting record procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a(j)(2), (k)(1) and/or (k)(2).

To the extent that this system is not subject to exemption, it is subject to contest. A determination as to exemption shall be made at the time a request for contest is received. Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager (See Appendix) stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in this system include, but are not limited to, investigation reports of federal, state and local law enforcement agencies; client agencies of the Department of Justice; other non-Department of Justice investigative agencies; forensic reports; statements of witnesses and parties; verbatim transcripts of Grand Jury and court proceedings; data memoranda and reports from the Court and agencies thereof; and the work product of Assistant United States Attorneys, Department of Justice attorneys and staff, and legal assistants working on particular cases.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsection (c) (3) and (4), (d), (e) and (3), (e)(4) (G) and (H), (e) (5) and (8), and (g) of the Privacy Act pursuant to 5 U.S.C. (j)(2) and (k) (1) and (2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/USA-009

System name:

Kline—District of Columbia and Maryland—Stock and Land Fraud Interrelationship Filings

System.

System location:

U.S. Attorney's Office, Judiciary Center Bldg., 555 4th Street, NW, Washington, DC 200

Categories of individuals covered by the system:

The individuals on whom records are maintained in this system may be broadly classified into three categories: (1) Those individuals who have been charged with Federal and D.C. Code violations; (2) Those individuals who are currently under investigation for violations of Federal and D.C. Code; (3) Those individuals upon whom investigations were conducted, but no prosecution was initiated. These include but are not limited to possible witnesses, corporate entities, corporate employees, business contacts, financial institutions and governmental contacts.

Categories of records in the system:

The system contains an index record for individual names and types of transactions with named individuals.

Authority for maintenance of the system:

5 U.S.C. 301, 28 U.S.C. 547, 23 D.C. Code 101(c).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of the record as follows:

(1) In any case in which there is an indication of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, the record in question may be disseminated to the appropriate agency, federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.

(2) In the course of investigating the potential or actual violation of any law, whether civil

criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation of a trial or hearing for such violation, a record may be disseminated to a federal, state, local, or foreign agency, or to an individual, if there is reason to believe that such agency or individual possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or informant;

(3) Records or extracts thereof relating to a case or matter may be disseminated to a defendant or his attorney or to the appropriate federal, state, local, or foreign, court or grand jury in accordance with established constitutional, substantive, or procedural law or practice;

(4) A record relating to a case or matter may be disseminated to a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing;

(5) A record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiations or discussion on such matters as settlement of a case or matter, plea bargaining, or informal discovery proceedings;

(6) A record relating to a case or matter that has been referred for investigation may be disseminated to the referring agency to notify such agency of the status of the case or matter or of any decision or determination that has been made;

(7) A record relating to a person held pending arraignment, trial or sentence, or after conviction, may be disseminated to a federal, state, local, or foreign prison, probation, parole, bail or pardon authority, or to any agency or individual concerned with the custody, maintenance, transportation, or release of such a person;

(8) A record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States;

(9) A record may be disseminated to a federal, state, local, or foreign law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency, or to provide investigative leads to such agency;

(10) A record may be disseminated to a federal agency, in response to its request, in

connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter; and

(11) A record may be accessed by volunteer student workers and students working under a college work-study program, as is necessary to enable them to perform their function.

(12) Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from system records maintained by the Department of Justice unless it is determined that release of specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(13) Release of information to Members of Congress. Information contained in systems or records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of the Member at the request of the individual who is the subject of the record and;

(14) Release of information to the National Archives and Records Administration (NARA) and the General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information maintained in the system is stored electronically in the Department of Justice System.

Retrievability:

Information is retrieved primarily by referencing the individuals' names who participated in business transactions.

Safeguards:

Information contained in this system is protected as though it was classified as confidential and accessible only to holders of the entry code: the only holders of the code are the U.S. Attorney's Offices for the District of Columbia and Maryland.

Retention and disposal:

The records are to be retained for the period of usefulness as determined by the U.S. Attorney's Office.

System manager(s) and address:

Chief, Fraud Division, U.S. Attorney's Office, Judiciary Center Bldg. 55 4th Street NW, Washington DC 20001.

Notification procedure:

All inquiries should be addressed to the System Manager.

Record access procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a. (j)(2), (k)(1), and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to access. A determination as to exemption shall be made at the time the request for access is received. A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request". Include in the request the general subject matter of the document or its file number. The requestor will also provide a return address for transmitting the information. Access request

will be directed to the System Manager listed above.

Contesting record procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a(j)(2), (k)(1), and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to contest. A determination as to exemption shall be made at the time a request for contest is received. Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Source of information contained in this system are individuals who have cooperated with U.S. Attorney's Office in the investigation of criminal activity.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(4)(G), and (H), (e)(5), and (8), (f), (g), and (h) of the Privacy Act pursuant to U.S.C. 552a(j)(2), and (k)(1) and (2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c), and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/USA-010

System name:

Major Crimes Division Investigative Files.

System location:

U.S. Attorney's Office, Judiciary Center Bldg., 555 4th St., NW, Washington, DC 20001.

Categories of individuals covered by the system:

The individuals on whom records are maintained in the Major Crimes Division Investigative System may be broadly classified in four categories: (1) Those individuals who have been charged with violations of Federal and D.C. Code; (2) those individuals who are currently under investigation for violations of Federal and D.C. Code; (3) those individuals upon whom investigations were conducted, but no prosecution was initiated; and (4) other informants.

Categories of records in the system:

In addition to the standard files maintained in accordance with the U.S. Attorney's Manual, the Department of Justice Docket and Reporting System, there are also maintained in the Major Crimes Division of this office certain investigative and intelligence files. The type of information maintained is identifying data, criminal records, intelligence compiled for the purpose of investigation of criminal offenses, criminal investigative reports, informant descriptions, summaries, and information provided in confidence during investigative and prosecutive phases of criminal cases.

Authority for maintenance of the system:

5. U.S.C. 301, 28 U.S.C. 547.23 D.C. Code 101(c).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of the record as follows:

(1) In any case in which there is an indication of a violation or potential violation of law, whether civil, criminal or regulatory in nature, the record in question may be disseminated to the appropriate agency, federal, state local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law.

(2) In the course of investigating the potential or actual violation of any law, whether civil, criminal or regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing for such violation, a record may be disseminated to a federal, state, local or foreign agency, or to an individual, if there is reason to believe that such agency or individual possesses information relating to the investigation, trial, or hearing and the dissemination of such information is necessary for the investigation, trial, or hearing.

reasonably necessary to elicit such information or to obtain the cooperation of a witness informant.

(3) Records or extracts thereof relating to a case or matter may be disseminated to a defendant or his attorney or to the appropriate federal, state, local or foreign, court or grand jury in accordance with established constitutional, substantive, or procedural law or practice;

(4) A record relating to a case or matter may be disseminated to a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing;

(5) A record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion on such matters as settlement of a case or matter, plea bargaining, or informal discovery proceedings;

(6) A record relating to a case or matter that has been referred for investigation may be disseminated to the referring agency to notify such agency of the status of the case or matter or of any decision or determination that has been made;

(7) A record relating to a person held pending arraignment, trial or sentence, or after conviction, may be disseminated to a federal, state, local, or foreign prison, probation, parole, bail or pardon authority, or to any agency or individual concerned with the custody, maintenance, transportation, or release of such a person;

(8) A record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States;

(9) A record may be disseminated to a federal, state, local, or foreign law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency;

(10) A record may be disseminated to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter; and

(11) A record may be accessed by volunteer student workers and students working under a college work-study program, as is necessary to enable them to perform their function.

(12) Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from system records maintained by the Department of Justice unless it is determined that release of specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(13) Release of information to Members of Congress: Information contained in systems records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of the individual who is the subject of the record and;

(14) Release of information to the National Archives and Records Administration (NARA) and the General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

The information is maintained in memorandum form in file folders.

Retrievability:

Information is retrieved primarily by the name of a person, complaint number, court document number, FBI number, Metropolitan Police Department identification number and District of Columbia Department of Corrections number.

Safeguards:

Information contained in the system is both unclassified and classified and is safeguarded by being maintained in tumbler locked file safes in the Major Crimes Division, which is manned during all times that it is open and at other times is locked. This room is located in the U.S. Courthouse which is guarded by the Federal Protective Service twenty four hours a day with roving patrols during non-working hours.

Retention and disposal:

Files are retained and disposed of in accordance with Title 8, U.S. Attorney's Manual, pages 70-77.

System manager(s) and address:

Chief, Major Crimes Division, U.S. Attorney's Office, Judiciary Center Bldg., 555 4th Street NW, Washington, DC 20001.

Notification procedure:

Address inquiries to the System Manager.

Record access procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a(j)(2), (k)(1), and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to access. A determination as to exemption shall be made at the request for access is received. A request for access to a record from this system shall be in writing, with the envelope and the letter clearly marked 'Privacy Access Request.' Include in the request the general subject matter of the document or its file number. The requestor also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a(j)(2), (k)(1), and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to contest. A determination as to exemption shall be made at the time a request for contest is received. Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendments to the information sought.

Record source categories:

Sources of information contained in this system are investigative reports of federal, state and local law enforcement agencies, statement of witnesses, informants and parties, as well as verbatim transcripts of grand jury proceedings and court proceedings, memoranda and correspondence from the court and agencies thereof and the work product of Assistant United States Attorneys and legal assistants working on particular cases.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsection (c) (3) and (4), (d), (e) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), (g) and (h) of the Privacy Act pursuant to U.S.C. 552a(j)(2) and (k) (1) and (2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/USA-011

System name:

Prosecutor's Management Information System (PROMIS).

System location:

U.S. Attorney's Office: Judiciary Center Bldg., 555 4th Street, NW, Washington, DC 200

Categories of individuals covered by the system:

The individuals on whom records are maintained in PROMIS are as follows: (1) Those individuals who have been charged with criminal violations: (2) those individuals who are currently under investigation for criminal violations: (3) those individuals upon whom criminal investigations were conducted, but no prosecution was initiated; and (4) the names and addresses of all witnesses and arresting police officers.

Categories of records in the system:

The data in PROMIS fall into six major categories.

1. Information about the accused or defendant. This includes name, alias, sex, race, date of birth, address, facts about prior arrest and convictions, and employment status. If judge appropriate, additional data could be added, such as information about alcohol or drug use. Some of this information is used to rate the gravity of the case in terms of the defendant's criminal history.
2. Information about the crime. The date, time, and place of the crime; the number of persons involved in the crime; and a numerical rating reflecting the gravity of the crime in terms of amount and degree of personal injury, property damage or loss, and intimidation.
3. Information about the arrest. The date, time, and place of the arrest, the type of arrest, and the identity of the arresting officers.
4. Information about criminal charges. The charges originally placed by the police against the arrestee, the charges actually filed in court against the defendant, the reasons for changing the charges by the prosecutor, the penal statute for the charge, the FBI Uniform Crime Code for the charge, and the Project SEARCH Code for the charge.
5. Information about court events. The dates of every court event in a case from arraignment through motion hearing, continuance hearing, final disposition, and sentencing; the names of the principals involved in each event, including the defense and prosecution attorneys and the judge; the outcomes of the events and the reasons therefor.
6. Information about witnesses. The names and addresses, the prosecutor's assessment

whether the witnesses are essential to the case, and any indications of reluctance to test the witnesses.

Authority for maintenance of the system:

5 U.S.C. 301, 28 U.S.C. 547, 23 D.C. Code 101(c).

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use by records as follows:

(1) In any case in which there is an indication of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, the record in question may be disseminated to the appropriate agency federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law;

(2) In the course of investigating the potential or actual violation of any law, whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation of a trial or hearing for such violation, a record may be disseminated to a federal, state, local, or foreign agency, or to an individual, if there is reason to believe that such agency or individual possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or informant;

(3) Records or extracts thereof relating to a case or matter may be disseminated to a defendant or his attorney or to the appropriate federal, state, local, or foreign, court or grand jury in accordance with established constitutional, substantive, or procedural law or practice;

(4) A record relating to a case or matter may be disseminated to a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing;

(5) A record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion on such matters as settlement of a case or matter, plea bargaining, or informal discovery proceedings, or to the Public Defender.

Service in connection with caseload management of other purposes;

(6) A record relating to a case or matter that has been referred for investigation may be disseminated to the referring agency to notify such agency of the status of the case or of any decision or determination that has been made or to assist in eliciting additional information;

(7) A record relating to a person held pending arraignment, trial or sentence, or after conviction, may be disseminated to a federal, state, local or foreign prison, probation, parole, bail or pardon authority, or to any agency or individual concerned with the custody, maintenance, transportation, or release of such a person;

(8) A record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States;

(9) A record may be disseminated to a federal, state, local, or foreign law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency;

(10) A record may be disseminated to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter; and

(11) A record may be accessed by volunteer student workers and students working under a college work-study program, as is necessary to enable them to perform their function.

(12) This office utilizes it to track the workload of the criminal court process from three vantage points. First, the workload is tracked from the vantage point of the crime or criminal incident. This is accomplished by including in PROMIS the complaint number which the department assigns to a reported crime. With this number, prosecutors can follow the full history of the court actions arising from the crime even though those actions may involve multiple defendants, multiple cases, and multiple trials and dispositions.

(13) PROMIS tracks the court workload from the vantage point of the accused or defense

This is achieved by incorporating in PROMIS the fingerprint-based number the police department assigns to the individual following his or her arrest. This identification number is used again by the department if the same individual is subsequently arrested. Through this number, prosecuting attorneys accumulate criminal history files on offenders and note incidents of recidivism.

(14) PROMIS tracks from the vantage point of the court proceedings. This is accomplished by including in PROMIS the docket number the Court assigns to the case pending before it. With this number, prosecutors trace the history of any formal criminal action from arraignment through final disposition and sentencing, and account for the separate fate of each count or charge.

The inclusion of these three numbers is significant. The numbers provide a capability to link the criminal incident, the defendant, or the court actions and provide the basis for the communication among the various Federal, state, local, and foreign law enforcement agencies.

(15) PROMIS generates, on a recurring basis, five categories of reports: Misdemeanor calendars, felony calendars, case status reports, workload reports, and special reports. These reports are prepared from information contained in the data base both by persons employed by this office, the Justice Department and persons under contract to the Department for this purpose.

(16) Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from system records maintained by the Department of Justice unless it is determined that release of specific information in the context of the particular case would constitute an unwarranted invasion of personal privacy.

(17) Release of information to Members of Congress. Information contained in systems or records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of the individual who is the subject of the record; and

(18) Release of information to the National Archives and Records Administration (NARA) and the General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to NARA and GSA in records management inspections conducted

under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

These records are stored on magnetic tapes and discs at the District of Columbia Metropolitan Police Department Computer Center. Printouts from the terminals are stored with case files. Status, calendars, and statistical reports are stored in the files and offices of supervisors and attorneys.

Retrievability:

This system has an on-line data retrieval capability with respect to certain information continued in the data base. These subsets of information are retrieved on data display terminals which are located at various work stations throughout the office. Certain of the terminals have a printout capability. All information on these subsets is a matter of public record. The system also has the capability for the production of periodic reports. Both the periodic reports and the on-line displays are utilized in accordance with the above listed uses.

Safeguards:

The magnetic tapes and discs are maintained in a secure vault at the Metropolitan Police Department Computer Center. In addition to the physical security safeguards, there is a twenty-four hour patrol. The data display terminals are located in semi-public areas of the office (i.e., administrative work stations through which the public must pass on official business). However, only trained operators may retrieve the information, which is of public concern.

record. The terminals are not open to the public after working hours.

Retention and disposal:

The files are retained and disposed of in accordance with Title 8, U.S. Attorney's Manual pages 70–77.

System manager(s) and address:

Administrative Assistant, United States Attorney, Judiciary Center Bldg., 555 4th St. NW
Washington, DC 20001.

Notification procedure:

Address inquiries to the System Manager.

Record access procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a(j)(2), (k)(1) and/or (j)(2). To the extent that this system is not subject to exemption, it is subject to access. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." Include in the request the general subject matter of the document or its file number. The requester shall also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a(j)(2), (k)(1) and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to contest. A determination as to exemption shall be made at the time a request for contest is received. Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

About 80 percent of the data contained in PROMIS is obtained at the intake and screen stage as the by-product of the case documentation process. Carbon copies of various forms completed immediately before or during the case screening stage serve as input documents to PROMIS.

As a case moves through the subsequent proceedings, additional information about its status is fed to PROMIS. This is achieved through turnaround documents—forms generated by PROMIS in advance of a court event—on which the results of a given processing (e.g., preliminary hearing, sentencing, etc.) are recorded and then entered in PROMIS.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c) (3) and (4), (d), (e) (2) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), (g) and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k) (1) and (2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/USA-012

System name:

Security Clearance Forms for Grand Jury Reports.

System location:

Ninety-four United States Attorney's Office (See attached Appendix).

Categories of individuals covered by the system:

Proposed Grand Jury Reporters.

Categories of records in the system:

Request for security clearance of grand jury reporter(s) employed by the reporting firm in contract with the Justice Department; carbon copy of "PERSONNEL INFORMATION SHEET—Grand Jury Reporting" on which is listed name of proposed grand jury reporter, address, date and place of birth, and present business affiliation; and clearance or denial of clearance for the proposed reporter from the Department of Justice.

Authority for maintenance of the system:

5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

All uses of this information are internal within the Department of Justice.

Release of information to the news media:

Information permitted to be released to the news media and the public pursuant to 28 C.F.R. 50.2 may be made available from systems of records maintained by the Department of Justice, unless it is determined that release of the specific information in the context of a particular request would constitute an unwarranted invasion of personal privacy.

Release of information to members of congress:

Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of 5 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose

relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Security clearance forms are kept alphabetically in file cabinets in the Administrative Office.

Retrievability:

Security clearance forms on grand jury reports are retrievable from an alphabetical filing system.

Safeguards:

Security clearance forms are maintained in the Administrative Division in the District Court Building which is manned at all times during working hours and at other times is locked.

Retention and disposal:

Security clearance forms are maintained for five years, at which time they must be renewed. Upon receipt of renewed security clearance, old forms are destroyed.

System manager(s) and address:

Ninety-four United States Attorneys Offices (See attached appendix).

Notification procedure:

Address inquiries to the System Manager.

Record access procedures:

A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." Include in the request the general subject matter of the document. The requestor will also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

The source of the information contained in these files are the reporter's request for security clearance personnel information sheet and the clearance or denial of clearance.

Systems exempted from certain provisions of the act:

None.

[\[TOP\]](#)

JUSTICE/USA-013

System name:

U.S. Attorney, District of Columbia Superior Court Operations, Criminal Files, including limited to the following subsystems: (a) Criminal File Folder (USA-S1), (b) Criminal File (USA-33), (c) Criminal Docket Card (USA-T7), and (d) Index.

System location:

U.S. Attorney's Office, Judiciary Center Bldg., 555 4th St. NW, Washington, DC 20001.

Categories of individuals covered by the system:

The individuals on whom records are maintained may be broadly classified in three categories: (1) Those individuals who have been charged with criminal violations; (2) those individuals who are currently under investigation for criminal violations; and (3) those individuals upon whom criminal investigations were conducted, but no prosecution was initiated.

Categories of records in the system:

This system of records, consisting of numbered Criminal File Folders, (USA-S1 and USA-S2) contains criminal investigative reports about named individuals submitted to this office by federal, state, local and foreign law enforcement agencies involved with the investigation of suspected violations as well as by complaints made by private parties. Those matters which become cases either by way of indictment or information in addition to the data contained in the investigative reports, also contain copies of indictments, informations, complaints, and pleadings submitted to the court in connection with the actual prosecution of the case. The files also contain communications between the Court and agencies thereof, and the United States Attorney, and all correspondence relative to the case or matter. The files further contain psychiatric, chemical and other forensic reports, documentary evidence and the work product and internal memoranda of the Assistant United States Attorney in charge of the investigation compiled in preparation for the prosecution of each case. In those cases which have gone through trial and appeal, the file would further reflect transcripts of the trial, all pleading correspondence between the attorneys and the Court of Appeals, and copies of briefs submitted in the prosecution of the Appeal.

A synopsis record of a matter or case is maintained by means of a criminal docket card (USA-T7), for all actions through sentencing. A synopsis record of a case on appeal is maintained on an Appellate Docket Card (USA-9X-199), Appellate Proceedings). All of the subsystems comprise an internal cross-reference record keeping system of the criminal business at the office. Through the medium of forms and on-line data input, certain of the information is conveyed to a computer center for inclusion in the Prosecutor's Management Information System (a system which will be reported on separately), from which status and statistical reports are issued and distributed back to this office either in the form of computer printouts or on data display terminals which contain much of the same information as the files in different format.

Because of the number of diverse functions which must be performed with respect to ex-

case; and because of the large volume of cases and because operations are conducted in three separate buildings, there are a number of file folder locator mechanisms and cross references utilized to constantly track a file folder when it is not physically located in file control. These indexes or locators are maintained in the form of 'out cards,' log books or card files, etc. They are referenced by name, number, and other identifiers. In themselves are not separate systems of records, but indexes or references to the primary system.

Authority for maintenance of the system:

5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of a record as follows:

- (1) In any case in which there is an indication of a violation or potential violation of law, whether civil, criminal, or regulatory in nature, the record in question may be disseminated to the appropriate agency, federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law;
- (2) In the course of investigating the potential or actual violation of any law, whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation of a trial or hearing for such violation, a record may be disseminated to a federal, state, local, or foreign agency, or to an individual, if there is reason to believe that such agency or individual possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or informant;
- (3) Records or extracts thereof relating to a case or matter may be disseminated to a defendant or his attorney or to the appropriate federal, state, local, or foreign, court or grand jury in accordance with established constitutional, substantive, or procedural law or practice;
- (4) A record relating to a case or matter may be disseminated to a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing;

(5) A record relating to a case or matter may be disseminated to an actual or potential prosecutor or his attorney for the purpose of negotiation or discussion on such matters as settlement of a case or matter, plea bargaining, or informal discovery proceedings;

(6) A record relating to a case or matter that has been referred for investigation may be disseminated to the referring agency to notify such agency of the status of the case or matter or of any decision or determination that has been made or to assist in eliciting additional information;

(7) A record relating to a person held pending arraignment, trial or sentence, or after conviction, may be disseminated to a federal, state, local, or foreign prison, probation, parole, bail or pardon authority, or to any agency or individual concerned with the custody, maintenance, transportation or release of such a person;

(8) A record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States;

(9) A record may be disseminated to a federal, state, local, or foreign law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency;

(10) A record may be disseminated to a federal agency, in response to its request, in connection with the hiring or retention of employee, the issuance of a security clearance, reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter; and

(11) A record may be assessed by volunteer student workers and students working under a college work-study program, as is necessary to enable them to perform their function;

(12) Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available for system records maintained by the Department of Justice unless it is determined that release of specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(13) Release of information to Members of Congress. Information contained in systems or records maintained by the Department of Justice, not otherwise required to be released pursuant to 5 U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests for information on behalf of the individual who is the subject of the record; and

(14) Release of information to the National Archives and Records Administration (NARA) or the General Services Administration (GSA): A record from a system of records may be disclosed as a routine use to NARA and GSA in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

The information in the various indexes is maintained on index cards, log books, out cards, and other documents. The criminal files themselves are maintained in criminal file folders (USA-S1 and USA-S2). Synopsis information is maintained on a Criminal Docket Card (USA-T7) and Appellate Proceedings (USA-9X-199).

Retrievability:

Information is retrieved primarily by the name of a person, complaint number, court document number, FBI number, Metropolitan Police Department identification number and District of Columbia Department of Corrections number.

Safeguards:

Information contained in the system is both unclassified and classified and is safeguard protected by being maintained in filerooms which are manned during all times that they open and at other times are locked. These rooms are located in the Superior Court for the District of Columbia, Buildings B and G which are guarded by the federal protective service twenty-four hours a day with roving patrols during non-working hours. Files which are not in the filerooms but which are checked out to attorneys are maintained in locked offices at all working hours.

Retention and disposal:

The files are retained and disposed of in accordance with Title 8, U.S. Attorney's Manual, pages 70–77.

System manager(s) and address:

Administrative Officer, U.S. Attorney's Office, Superior Court Operations, 555 4th Street, N.W., Washington, DC 20001.

Notification procedure:

Address inquiries to the System Manager.

Record access procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a(j)(2), (k)(1) and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to access. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." Include in the request the general subject matter of the document or its file number. The requester shall also provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above.

Contesting record procedures:

The major part of the information maintained in this system is exempt from this requirement

under 5 U.S.C. 552a(j)(2), (k)(1) and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to contest. A determination as to exemption shall be made at the time a request for contest is received. Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in this system include but are not limited to investigative reports of federal, state and local law enforcement agencies, forensic reports, statements of witnesses and parties, as well as verbatim transcripts of grand jury proceedings and court proceedings, memoranda and reports from the court and agencies thereof and work product of Assistant United States Attorney and legal assistants working on particular cases.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c) (3) and (4), (d), (e) (2) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), (g), and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k) (1) and (2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 533 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/USA-014

System name:

Pre-Trial Diversion Program Files.

System location:

Ninety-four United States Attorneys' Offices (See attached appendix).

Categories of individuals covered by the system:

Individuals referred to in potential or actual pre-trial diversion cases.

Categories of records in the system:

(a) USA Form 184—Referral letter to Probation Service; (b) USA Form 185—Letter to defendant; (c) USA Form 186—Agreement for Pre-Trial Diversion; (d) USA Form 187—Pre-Trial Diversion Report Form; (e) USA Form 188—Certification of Completion of Program; (f) USA Form 189—Defendant Application Form; (g) Telephone Records; (h) Miscellaneous Correspondence; and (i) Files Unique to a District.

Authority for maintenance of the system:

This system is established and maintained pursuant to 5 USC 301 and 44 USC 3101.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in this system of records may be disseminated as a routine use of a record as follows:

(a) In any case in which there is an indication of a violation or potential violation of law criminal or regulatory in nature, the record in question may be disseminated to the appropriate Federal, state, local, or foreign agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(b) In the course of investigating the potential or actual violation of any law, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing for such violation, a record may be disseminated to a Federal, state, local, or foreign agency, or to an individual or organization, if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant;

(c) A record relating to a case or matter may be disseminated in an appropriate Federal, state, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practice;

(d) A record relating to a case or matter may be disseminated to a Federal, state, or local

administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing;

(e) A record relating to a case or matter be disseminated to an actual or potential party or attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining, or informal discovery proceedings;

(f) A record relating to a case or matter that has been referred by an agency for investigation or prosecution or enforcement, or that involves a case or matter within the jurisdiction of an agency, may be disseminated to such agency to notify the agency of the status of the case or matter of any decision or determination that has been made, or to make such other inquiries and reports as are necessary during the processing of the case or matter;

(g) A record relating to a person held in custody pending or during arraignment, trial, sentencing, or extradition proceedings, or after conviction or after extradition proceedings, may be disseminated to a Federal, state, local, or foreign prison, probation, parole, or pardon authority or to any other agency or individual concerned with the maintenance, transportation, or care of such a person;

(h) A record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States or to an executive agreement;

(i) A record may be disseminated to a Federal, state, local, foreign, or international law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigation leads to such agency;

(j) A record may be disseminated to a Federal agency, in response to its request in connection with the hiring or retention of an employee, the issuance of a security clearance, the request for an investigation of an employee, the letting of a contract, or the issuance of a license or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter;

(k) A record may be disseminated to the public, news media, trade associations, or other groups, when the purpose of the dissemination is educational or informational, such as descriptions of crime trends or distinctive or unique modus operandi, provided that the record

does not contain any information identifiable to a specific individual;

(l) A record may be disseminated to a foreign country, through the United States Department of State or directly to the representative of such country, to the extent necessary to assist such country in apprehending and/or returning a fugitive to a jurisdiction which seeks his return;

(m) A record that contains classified national security information and material may be disseminated to persons who are engaged in historical research projects, or who have previously occupied policy making positions to which they were appointed by the President in accordance with the provisions codified in 28 CFR 17.60; and

(n) A record may be accessed by volunteer student workers and students working under a college work-study program, as is necessary to enable them to perform their function.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

All information, except that specified in this paragraph, is recorded on basic paper/card material, and stored within manila file folders, within metal file cabinets, electric file/card retrievers or safes. Some material is recorded and stored on magnetic tape, card or other processing type storage matter for reproduction later into conventional formats.

Retrievability:

Information is retrieved by the name of the person, case number or complaint number.

Safeguards:

Information in the system is both confidential and nonconfidential and located in file cabinets at the United States Attorney offices. Some materials are located in locked file drawers and others in unlocked file drawers. Offices are locked during nonworking hours and are secured by either Federal Protective Service, United States Postal Service, or private bodyguards.

Retention and disposal:

Records are maintained and disposed of in accordance with Department of Justice retention plans.

System manager(s) and address:

System Manager for the system in each office is the Administrative Officer/Assistant, for U.S. Attorney for each district. (See attached appendix.)

Notification procedure:

Address inquiries to the System Manager for the judicial district in which the diversion application or approval was made. (See attached appendix.)

Record access procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a(j)(2), (k)(1) and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to access. A determination as to exemption shall be made at the time a request for access is received. A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly marked "Privacy Access Request." Include in the request the name of the individual involved, his birth date and place, or any other identifying number or information which may be of assistance in locating the record and the name of the case or matter involved, if known. The requester shall also provide a return

address for transmitting the information. Access requests will be directed to the System Manager. (See attached appendix.)

Contesting record procedures:

The major part of the information maintained in this system is exempt from this requirement under 5 U.S.C. 552a(j)(2), (k)(1) and/or (k)(2). To the extent that this system is not subject to exemption, it is subject to contest. A determination as to exemption shall be made at the time a request for contest is received. Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager (see attached appendix) stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in this system include, but are not limited to investigative reports of Federal, state and local law enforcement agencies; client agencies of the Department of Justice; other non-Department of Justice investigative agencies; forensic reports; statements of witnesses and parties; verbatim transcripts of Grand Jury and court proceedings; data; memoranda and reports from the Court and agencies thereof; and the product of Assistant United States Attorneys, Department of Justice attorneys and staff, legal assistants working on particular cases.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c) (3) and (4), (d), (e) (2) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), (g) and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k) (1) and (2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/USA-015

System Name:

Debt Collection Enforcement System, JUSTICE/USA-015.

Security Classification:

Sensitive but unclassified.

System Location:

The Executive Office for United States Attorneys ("EOUSA") in Washington, DC, the National Operations Center ("NOC") in Columbia, SC, and individual United States Attorneys' Offices ("USAOs") and their agents in each of the 94 Federal judicial districts nationwide, depend upon where debt collection proceedings are pending. (Individual office addresses can be located on the Internet at <http://www.usdoj.gov/usao>.)

Categories of Individuals Covered By the System:

Individuals indebted to the United States who have either: (1) Allowed their debts to become delinquent and whose delinquent debts have been assigned to a USAO, or to private counsel retained by DOJ pursuant to contract ("contract private counsel"), for settlement or enforcement collection through litigation; and/or (2) incurred debts assessed by a Federal court, e.g., or penalties in connection with civil or criminal proceedings.

Categories of Records in the System:

This system of records contains records relating to the negotiation, compromise, settlement and litigation of debts owed the United States. Records consist of debt collection case files as well as automated and/or hard-copy supporting data, as summarized below.

Case files include: evidence of indebtedness, judgment, or discharge; court filings such as legal briefs, pleadings, judgments, orders, and settlement agreements; litigation reports; related attorney work product; and agency status reports, memoranda, correspondence and other documentation developed during the negotiation, compromise, settlement and/or litigation of debt collection activities.

Automated and/or hard-copy supporting data include information extracted from the case files and information generated or developed in support of Federal debt collection activities. This information may include: Personal data (e.g., name, social security number, date of birth, taxpayer identification number, locator information, etc.); claim details (e.g., value and type of claim); and information regarding the status of the claim.

claim, such as benefit overpayment, loan default, bankruptcy, etc.); demand information settlement negotiations, and compromise offered; account information (e.g., debtor's payments, including principal, penalties, interests, and balances, etc.); information regarding debtor's employment, ability to pay, property liens, etc.; data regarding debtor's loans or benefits from client agencies or other entities; information on the status and disposition of cases at various times; and any other information related to the negotiation, compromise, settlement, or litigation of debts owed the United States, or to the administrative management of debt collection efforts.

Authority For Maintenance of the System:

This system is established and maintained pursuant to the Debt Collection Act of 1982, Law 97–365, 96 Stat. 1749 (1982), as amended by the Debt Collection Improvement Act of 1996, Public Law 104–134, 110 Stat. 132 (1996) (codified at 31 U.S.C. 3701, *et seq.*); the Federal Debt Collection Procedure Act of 1990, Public Law 101–647, 104 Stat. 4933 (1990) (codified at 28 U.S.C. 3001, *et seq.*); the Cash Management Improvement Act of 1992, as amended by Public Law 102–589, 106 Stat. 5135 (1994); and related authority.

Purposes:

This system of records is maintained by EOUSA to cover records used by the USAOs, and contract private counsel, to perform legal services associated with the collection of debt due the United States—including related negotiation, settlement, litigation, and enforcement efforts—in accordance with the Debt Collection Act and related authority. More specifically, 31 U.S.C. 3711 authorizes the Attorney General to conduct litigation to collect delinquent debts due the United States. In addition, 31 U.S.C. 3718(b) authorizes the Attorney General to contract with private counsel to assist DOJ in collecting debts due the United States. The Attorney General is further authorized by 28 U.S.C. 3101 and 3201, *et seq.* (Chapter 17 "Federal Debt Collection Procedure") to obtain both pre-judgment and post-judgment remedies against delinquent debtors. Moreover, under 28 U.S.C. 3201(a) and (e), a judgment against such a debtor creates a lien on all real property of the debtor, and renders that property ineligible for any grant or loan insured, financed, guaranteed, or made by the Federal Government.

Note:

A separate but ancillary system of records—entitled "Debt Collection Management System"

Justice/JMD-006" —is maintained by the Justice Management Division ("JMD"). System JMD-006 furnishes automated litigation and/or administrative support to USAOs and to contract private counsel to assist in Federal debt collection activities. In addition, the JMD system maintains an inventory of debtor files in all 94 judicial districts, consisting of all cases referred to DOJ for settlement and/or enforced collection through litigation. The inventory enables DOJ to provide statistical data to Congress and OMB on debt collection in accordance with 31 U.S.C. 3718(c).

***Routine Uses Of Records Maintained In The System, Including Categories Of Users
Purposes Of Such Uses:***

1. Disclosures to Former Employees

Information may be disclosed to a former employee of the Department for purposes of: responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

2. Disclosures to Contractors and Other Personnel

Information may be disclosed to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records, including but not limited to persons assigned to the Department's Nationwide Central Intake Facility ("NCIF") and/or contract private counsel and their agents.

3. Disclosures Related to Offsets and Remedies

Information may be disclosed to the Internal Revenue Service ("IRS"), Department of Defense ("DOD"), United States Postal Service ("USPS"), and/or Department of Housing and Urban Development ("HUD") in accordance with computer matching or data sharing programs to locate debtors eligible for Federal tax refunds, salaries, pensions, annuities, benefits, or Federal payments against which offsets or other remedies would be appropriate. The data and associated records of individuals so identified may be referred to the appropriate Federal

agency for collection by administrative, salary, or other procedures to offset Federal pay

4. Disclosures to Treasury Department

Information may be disclosed to the Department of the Treasury, including the IRS, pursuant to the Debt Collection Improvement Act and related authority for any purpose related to debt collection, including locating debtors for debt collection efforts and/or effecting offsets against monies payable to such debtors by the Federal Government.

5. Disclosures to Client Agencies

Information from this system may be disclosed to client agencies who have referred outstanding debts to DOJ for debt collection efforts, including settlement or litigation, to such agencies of case developments, the status of accounts receivable or payable, case-related decisions or determinations, or to make such other inquiries and reports related to debt collection efforts.

6. Disclosures to Disbursing/Offset Agencies

Information from this system may be disclosed to any Federal agency that employs and pays pension, annuity and/or other benefits to an individual who has been identified as delinquent debtor for purposes of offsetting the individual's salary and/or pension, annuity, or other benefit payment received from that agency, when DOJ is responsible for the enforcement of collection of a judgment or claim on behalf of the United States against that person.

7. Disclosures for Debt Verification and Collection Purposes

Information from this system may be disclosed to any Federal, State, local, or tribal agency to an individual or organization, if there is reason to believe that they possess information relating to the verification or collection of debts owed the Federal Government, and if the disclosure seeks to elicit information from such entities regarding: (a) The status of such debts, including settlement, litigation, or other collection efforts; (b) the identification or location of such debtors; or (c) the cooperation of witnesses, informants, or others possessing collection-related information.

8. Disclosures of Non-Tax Debts

In accordance with regulations issued by the Secretary of the Treasury to implement the

Collection Improvement Act of 1996, information from this system may be disclosed to p or otherwise publicly disseminate the identity of debtors and/or the existence of non-tax in order to direct actions under the law toward delinquent debtors that have assets or in sufficient to pay their delinquent non-tax debts, but only: upon taking reasonable steps ensure the accuracy of the identity of a debtor; upon ensuring that such debtor has had opportunity to verify, contest, and compromise a non-tax debt; and with the review of the Secretary of Treasury or designee.

9. Disclosures for Audit, Oversight, and Training

Information from this system may be disclosed to any individual or organization requiring information for the purpose of performing audit, oversight, and training operations of DC to meet related reporting requirements.

10. Disclosures to Law Enforcement and Regulatory Agencies

Where a record, either on its face or in conjunction with other information, indicates a vi or potential violation of law—criminal, civil, or regulatory in nature—the relevant records referred to the appropriate Federal, State, local, foreign, or tribal, law enforcement auth other appropriate agency charged with the responsibility of investigating or prosecuting violation or enforcing or implementing such law.

11. Disclosures in Proceedings

Information from this system may be disclosed in an appropriate proceeding before a cc administrative or adjudicative body, when DOJ determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

12. Disclosures in Settlement/Plea Negotiations

Information from this system may be disclosed to an actual or potential party to litigation party's authorized representative for the purpose of negotiation or discussion of such m as settlement, plea bargaining, or in informal discovery proceedings.

13. Disclosures Related to Federal Employment, Clearance, Contracts, and Grants

Information from this system may be disclosed to appropriate officials and employees of Federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; letting of a contract, or the issuance of a grant or benefit.

14. Disclosures Related to State or Local Employment

Information from this system may be disclosed to designated officers and employees of local (including the District of Columbia), or tribal law enforcement or detention agency in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prison detainees, to the extent that the information is relevant and necessary to the recipient's decision.

15. Disclosures Related to Licenses and Permits

Information from this system may be disclosed to Federal, State, local, tribal, foreign, or international licensing agencies or entities which require information concerning the suitability or eligibility of an individual for a license or permit.

16. Disclosures to NARA

Information from this system may be disclosed to the National Archives and Records Administration ("NARA") for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

17. Disclosures to News Media and Public

Information from this system may be disclosed to the news media and the public pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

18. Disclosures to Members of Congress

Information from this system may be disclosed to a Member of Congress or staff acting

the Member's behalf when the Member or staff requests the information on behalf of, or the request of, the individual who is the subject of the record.

19. Disclosures Related to Health Care Fraud

Information from this system relating to health care fraud may be disclosed to private health plans, or associations of private health plans, and health insurers, or associations of health insurers, for the following purposes: To promote the coordination of efforts to prevent, detect, investigate, and prosecute health care fraud; to assist efforts by victims of health care fraud to obtain restitution; to enable private health plans to participate in local, regional, and national health care fraud task force activities; and to assist tribunals having jurisdiction over claims against private health plans.

20. Disclosures to Complainants and Victims

Information from this system may, in the agency's discretion, be disclosed to persons determined to be complainants and/or victims, to the extent deemed necessary to provide persons with information concerning the progress and/or results of the investigation or concerning matters arising from the matters of which they complained and/or of which they were a victim.

Disclosure To Consumer Reporting Agencies:

Information from this system of records may be disclosed to a credit or consumer report agency, as such terms are used in the Fair Credit Reporting Act (15 U.S.C. 1681, *et seq.*) or the Debt Collection Act (31 U.S.C. 3701, *et seq.*), when such information is necessary or relevant to Federal debt collection efforts, including, but not limited to, obtaining a credit report on a debtor, payor, or other party-in-interest; reporting on debts due the Government; or pursuing the collection of such debts through settlement, negotiation, or litigation.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing Records in the System:

Storage:

Certain records in this system are maintained in automated computer information system stored in electronic format for use or reproduction in report form at various times. Other records in this system are maintained in paper format located in file cabinets, safes, and similar

containers.

Retrievability:

Data in this system of records may be retrieved by debtor names or personal identifiers, numbers, computerized queries, and other keyword searches.

Safeguards:

Records contained in this system are unclassified. They are safeguarded and protected in accordance with DOJ rules and procedures governing the handling of office records and computerized information. Access to this system is restricted to those DOJ employees and contractors, including contract private counsel, who need access to perform official debt collection activities, including related administrative and support functions. During duty hours, access to this system is monitored and controlled by DOJ employees and contractors. During nonduty hours, records are maintained in locked facilities. Access to automated data requires the use of the proper password and user identification code. Access by contract private counsel is restricted to those cases assigned to them for debt collection efforts.

Retention and Disposal:

Records from this system are retained and disposed of in accordance with Part 3–13.31 United States Attorneys' Manual ("Comprehensive Retention Schedule") published at http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title3/13musa.htm, and related authority.

System Manager(S) and Address:

The system managers for this system of records are located at the Executive Office for United States Attorneys in Washington, DC, the Network Operations Center in Columbia, SC, and individual United States Attorneys' Offices in the 94 Federal judicial districts nationwide, depending upon where debt collection proceedings are pending. (Individual office addresses can be located on the Internet at <http://www.usdoj.gov/usao>.)

Notification Procedure:

Address inquiries to the System Manager (see above) in the judicial district where debt

collection efforts were initiated. For further information, see 28 CFR 16.40, *et seq.*

Record Access Procedure:

Requests for access must be in writing and should be addressed to the System Manager (see [System Manager](#) above) in the judicial district where debt collection efforts were initiated. The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.41 ("Requests for Access to Records"), *et seq.* Access requests must contain the requester's name, current address, date and place of birth, and should include a clear description of the records sought and any other information that would help to locate the record (e.g., name of the case and Federal agency to whom the debtor is indebted). Access requests must be signed and dated and either notarized or submitted under penalty of perjury pursuant to 18 U.S.C. 1746.

Contesting Record Procedures:

Individuals desiring to contest or amend information maintained in the system should clearly and concisely state what information is being contested, the reasons for contesting it, and the proposed amendment to the information. Address such inquiries to the System Manager (see [System Manager](#) above) in the judicial district where debt collection efforts were initiated. The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.46 ("Request for Amendment or Correction of Records"), *et seq.*

Record Source Categories:

Sources of information contained in this system primarily consist of the individuals covered by the system; DOJ and/or agencies to whom the individual is indebted, seeks benefits, or has furnished information; attorneys or other representatives of debtor and/or payors; and Federal, State, local, tribal, foreign, or private organizations or individuals who may have information regarding the debt, the debtor's ability to pay, or any other information relevant or necessary to assist in debt collection efforts.

Exemptions Claimed for the System:

None.

[\[TOP\]](#)

JUSTICE/USA-016

System name:

Assistant United States Attorney Applicant Records System.

System location:

Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

The system encompasses all applicants for Assistant United States Attorney positions.

Categories of records in the system:

This system of records consists of records folders which may contain up to a total of four sections. The personnel section contains records such as resumes, letters of recommendation, law school grade transcripts, completed Civil Service forms, and related personnel matters. The character section contains completed or portions of ongoing background investigations and matters related thereto. The Congressional section contains Congressional and other political type recommendations regarding appointment. The protest section contains correspondence, if any exists, protesting the appointment of applicants. Rarely does a personnel folder contain more than the personnel and character sections.

Authority for maintenance of the system:

These records are maintained pursuant to 5 U.S.C. 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records are used only by Department of Justice personnel for recruitment purposes. However, the fact that the applicant was being considered would be made known to the references supplied by the applicant and others contacted. Information about the applicant then known, might be supplied to contacted individuals as necessary to verify already o

information or to seek elaboration of that information.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Release of information to civil or criminal law enforcement agencies: Information may be disclosed to any civil or criminal law enforcement agency, whether Federal, State, local, or foreign, which requires information relevant to a civil or criminal investigation.

Release of information to agencies regarding the hiring or retention of employees; Information may be disclosed to officials and employees of the White House or any Federal agency which requires information relevant to an agency decision concerning the hiring, appointment, retention of an employee; the issuance of a security clearance; the execution of a security suitability investigation; the classification of a job; or the issuance of a grant or benefit.

Release of information to Federal, State, and local licensing agencies: Information may be disclosed to Federal, State, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

Release of information before a court or adjudicative body: Information may be disclosed in a proceeding before a court or adjudicative body before which the Office of the Deputy Attorney General (ODAG) is authorized to appear when (a) ODAG, or any subdivision thereof or

employee of ODAG in his or her official capacity, or (c) any employee of ODAG in his or individual capacity where the Department of Justice has agreed to represent the employee (d) the United States, where ODAG determines that the litigation is likely to affect it or a subdivisions, is a party to litigation or has an interest in litigation and such records are determined by ODAG to be arguably relevant to the litigation.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

These records are stored in paper folders.

Retrievability:

Information is retrieved by use of the applicant's name, as the folders are filed alphabetically by name.

Safeguards:

These records are maintained in cabinets stored in a locked room.

Retention and disposal:

These records are retained, in the case of applicants who are not offered positions, for two years and then destroyed. If the applicant is offered a position and accepts it, his folder is transferred to the Appointed Assistant United States Attorney Personnel System and retained as specified therein.

System manager(s) and address:

Associate Deputy Attorney General, Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Address all inquiries to the System Manager. These records will be exempted from subsections (d)(1) and (e)(1) of section 552a, Title 5, United States Code, by the Attorney General under the authority of 5 U.S.C. 552a(k)(5) to the extent therein permitted.

Record access procedures:

A request for access to non-exempt portions of records from this system should be clearly directed orally or in writing to the Associate Deputy Attorney General. When requests are in writing, the envelope and letter should be marked "Privacy Access Request."

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the Associate Deputy Attorney General, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information.

Record source categories:

Non-exempt sources of information contained in this system include the individual, government agencies as appropriate, and interested third parties.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (d)(1) and (e)(1) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/USA-017

System name:

Appointed Assistant United States Attorneys Personnel System.

System location:

Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue NW, Washington, DC 20530.

Categories of individuals covered by the system:

The system encompasses all Assistant United States Attorneys.

Categories of records in the system:

This system of records consists of records folders which may contain up to a total of five sections. The personnel section contains personnel records such as completed Civil Service forms, letters of recommendation, law school grade transcripts, appointment letters, appointment affidavits, bar affidavits, locator forms and personnel action forms. The character section contains completed or portions of ongoing background investigations and matters related thereto. The Congressional section contains Congressional and other political type recommendations regarding appointment. The protest section contains correspondence exists, protesting the appointment of applicants. The complaint section contains correspondence from individuals or groups complaining about office holders. Rarely does a personnel folder contain more than the personnel and character sections.

Authority for maintenance of the system:

These records are maintained pursuant to 5 U.S.C 301.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

These records are used only by Department of Justice personnel. Information contained in a folder may be used as the basis for answering future inquiries from other government agencies about a former assistant's qualifications. The personnel section may be made available to federal agencies, at their request, upon the transfer of the assistant to such an agency.

Release of information to the news media: Information permitted to be released to the news media and the public pursuant to 28 CFR 50.2 may be made available from systems of records maintained by the Department of Justice unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

Release of information to Members of Congress: Information contained in systems of records maintained by the Department of Justice, not otherwise required to be released pursuant to U.S.C. 552, may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of and at the request of the individual who is the subject of the record.

Release of information to the National Archives and Records Administration: A record from a system of records may be disclosed as a routine use to the National Archives and Records Administration (NARA) in records management inspections conducted under the authority of U.S.C. 2904 and 2906.

Release of information to civil or criminal law enforcement agencies: Information may be disclosed to any civil or criminal law enforcement agency, whether Federal, State, local, or foreign, which requires information relevant to a civil or criminal investigation.

Release of information to agencies regarding the hiring or retention of employees: Information may be disclosed to officials and employees of the White House or any Federal agency which requires information relevant to an agency decision concerning the hiring, appointment, retention of an employee; the issuance of a security clearance; the execution of a security suitability investigation; the classification of a job; or the issuance of a grant or benefit.

Release of information to Federal, State, and local licensing agencies: Information may be disclosed to Federal, State, and local licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

Release of information before a court or adjudicative body: Information may be disclosed in a proceeding before a court or adjudicative body before which the Office of the Deputy Attorney General (ODAG) is authorized to appear when (a) ODAG, or any subdivision thereof, or employee of ODAG in his or her official capacity, or (c) any employee of ODAG in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (d) the United States, where ODAG determines that the litigation is likely to affect it or a subdivision, is a party to litigation or has an interest in litigation and such records are determined by ODAG to be arguably relevant to the litigation.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

These records are stored in paper folders.

Retrievability:

Information is retrieved by use of the assistant's name, as the folders are filed alphabetically by name.

Safeguards:

These records are maintained in cabinets stored in a locked room.

Retention and disposal:

These records are retained until the subjects of the files resign or otherwise leave their employment.

for non-federal government employment. In that instance, the personnel section is sent to the St. Louis Records Center for an indefinite period. If the assistant transfers to another agency of the federal government, the personnel section is sent to the gaining agency. All other sections of the folder are destroyed six months after the assistant leaves office.

System manager(s) and address:

Associate Deputy Attorney General, Office of the Deputy Attorney General, United States Department of Justice, 10th and Constitution Avenue, NW, Washington, DC 20530.

Notification procedure:

Address all inquiries to the System Manager. These records will be exempted from subsections (d)(1) and (e)(1) of section 552a, Title 5, United States Code, by the Attorney General under the authority of 5 U.S.C. 552a(k)(5) to the extent therein permitted.

Record access procedures:

A request for access to non-exempt portions of records from this system should be directed orally or in writing to the System Manager. When requests are in writing, the envelope or letter should clearly be marked 'Privacy Access Request.'

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment(s) to the information.

Record source categories:

Sources of information contained in this system include the individuals, government agencies, as appropriate, and interested third parties.

Systems exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (d)(1) and (e)(1) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(5). Rules have been promulgated in accordance

the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/USA-018

System name:

United States Attorney's Office, *Giglio* Information Files.

System location:

Ninety-four United States Attorney's offices (see Appendix identified as Justice/USA-99 published 2-3-93 (58 FR 6983)) and offices posted on the Internet web site of the Executive Office for United States Attorneys (EOUSA) at <http://www.usdoj.gov/eousa>; and the EO U.S. Department of Justice, 950 Pennsylvania Avenue, NW, Washington, DC 20530.

Categories of individuals covered by the system:

Individuals who may serve as affiants or testify as witnesses in criminal proceedings brought by the ninety-four United States Attorneys' offices.

Categories of records in the system:

This system contains potential witness impeachment information including records of disciplinary actions. Records will include, but are not limited to: (a) Specific instances of witness conduct that may be used for the purpose of attacking the witness' credibility or character for truthfulness; (b) evidence in the form of opinion as to a witness' character or reputation for truthfulness; (c) prior inconsistent statements; and (d) information that may be used to suggest that a witness is biased. The system may also contain any judicial rulings, related pleadings, correspondence, or memoranda pertaining to the relevant criminal cases.

Authority for maintenance of the system:

This system is established and maintained under the authority of 5 U.S.C. 516 and 547.

Purpose(s):

This system has been established to enable the Department of Justice's prosecuting of maintain and disclose records of potential impeachment information from the Department investigative agencies, in accordance with *Giglio v. United States*, 405 U.S. 150 (1972).

It permits the United States Attorneys' offices to obtain information from federal and state agencies and to maintain and disclose for law enforcement purposes records of impeachment information that is material to the defense of federal criminal prosecutions.

Primary users of this system will be Requesting Officials, who are senior officials serving points of contact concerning potential impeachment information within each of the United States Attorneys' offices, and Assistant United States Attorneys who are prosecuting cases that have an obligation to disclose impeachment material under the *Giglio* decision.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

A record maintained in the system of records may be disseminated as a routine use of a record as follows:

- (a) A record will be provided to a court and/or defense attorney in satisfaction of the Department's obligations under the *Giglio* decision.
- (b) A record, or facts derived therefrom, may be disseminated in a proceeding before a judicial or adjudicative body before which the United States Attorney's office or the Executive Office for United States Attorneys is authorized to appear when (i) the United States Attorney's office or the Executive Office for United States Attorneys, or any subdivision thereof, or (ii) any employee of the United States Attorney's office or the Executive Office for United States Attorneys in his or her official capacity, or (iii) any employee of the United States Attorney's office or the Executive Office for United States Attorneys in his or her individual capacity, or (iv) the United States Attorney's office or the Executive Office for United States Attorneys determines that the litigation is likely to affect it or any subdivisions, is a party to litigation or has an interest in litigation and such records are determined by the United States Attorney's office or the Executive Office for United States Attorneys.

Attorneys to be arguably relevant to the litigation;

(c) In any case in which there is an indication of a violation or potential violation of law, criminal, civil, or regulatory in nature, the record in question may be disseminated to the appropriate federal, state, local, or foreign agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing the law;

(d) In the course of investigating any potential or actual violation of any law, criminal, civil, or regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing for such violation, a record may be disseminated to a federal, state, local, or foreign agency, or to an individual or organization, if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant;

(e) A record relating to a case or matter may be disseminated in connection with a federal, state, or local administrative or regulatory proceeding or hearing in accordance with the procedures governing such proceeding or hearing;

(f) A record relating to a case or matter may be disseminated in an appropriate federal, state, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practice;

(g) A record relating to a case or matter that has been referred by an agency for investigation, prosecution, or enforcement, or that involves a case or matter within the jurisdiction of an agency, may be disseminated to such agency to notify the agency of the status of the case or matter or of any decision or determination that has been made, or to make such other inquiries and reports as are necessary during the processing of the case or matter;

(h) Subject to the limitations of 28 CFR 50.2 and after a determination that release of the specific record in the context of a particular case would not constitute an unwarranted invasion of personal privacy, a record may be disseminated to the news media and public;

(i) Records not otherwise required to be released pursuant to 5 U.S.C. 552a may be made available to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests information on behalf of and at the request of the individual who is the

of the record;

(j) A record may be disclosed as a routine use to the National Archives and Records Administration (NARA) and to the General Services Administration (GSA) in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purpose responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Generally, all records are recorded on basic paper/cardboard material and stored in file cabinets. Some offices also may maintain the records in electronic format available through the Requesting Official's computer terminal.

Retrievability:

Records are retrieved primarily by the name of the prospective witness. A record within the system of records may be accessed within a United States Attorney's office by the Requesting Official or appropriate Assistant United States Attorney.

Safeguards:

Records in the system are confidential and are located in file cabinets in the United States Attorneys' offices. Offices are locked during non-working hours and are secured by either Federal Protective Service, the United States Postal Service, or in a private building with controlled access to the various United States Attorneys' offices and the Executive Office of the United States Attorneys. The ability to access electronically is restricted to those who have a valid ID and password. Authorized access is limited to those with a need-to-know and for

appropriate functions.

Retention and disposal:

Records are to be retained and disposed of in accordance with agency retention plans. records will also be maintained in accordance with the Attorney General's *Giglio* Policy in the United States Attorney's Manual, Title 9, paragraph 5.100. Potential impeachment information, together with any judicial rulings, related pleadings, and related correspondence or memoranda, will be placed in the office's *Giglio* Information File; copies will be provided to the agency official that provided the information and to the employing agency official for retention. When an employee has retired and any litigation pending in the prosecuting office in which the employee could be an affiant or witness is resolved, the Requesting Official shall remove any record that can be accessed by the identity of the employee.

System manager(s) and address:

System Manager for the system in each office is the *Giglio* Requesting Official, as defined in the United States Attorney's Manual, Title 9, paragraph 5.100, for the United States Attorney for each district (see Appendix USA-999 or EOUSA Internet addresses at <http://www.usdoj.gov/eousa>).

Notification procedure:

Address inquiries to the System Managers listed above.

Record access procedures:

Pursuant to 5 U.S.C. 552a(j)(2) and (k)(2), this record system has been exempted from public access provisions in 5 U.S.C. 552a(d).

Contesting recORDS PROCEDURE:

Pursuant to 5 U.S.C. 552a(j)(2) and (k)(2), this record system has been exempted from public record contesting provisions in 5 U.S.C. 552a(d)(3)–(4).

Record source categories:

Sources of records contained in this system include, but are not limited to, reports of federal

state and local law enforcement agencies; client agencies of the Department of Justice; non-Department of Justice investigative agencies; data, memoranda and reports from them and agencies thereof; and the work product of Assistant United States Attorneys, Department of Justice attorneys and staff, and legal assistants working on particular cases.

System exempted from certain provisions of the act:

The Attorney General has exempted this system from subsections (c)(4), (e)(2), (e)(5), and (f) of the Privacy Act, pursuant to 5 U.S.C. 552a(j)(2) and exempted this system from subsections (c)(3), (d), (e)(1), (e)(4)(G) and (H), and (f), pursuant to 5 U.S.C. 552a (j)(2) and (k)(2). These exemptions apply to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and (k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (c) and (e) and have been published in the *Federal Register* as of this date and proposed as additional to Title 28 Code of Federal Regulations (28 CFR part 16.81).

[\[TOP\]](#)

JUSTICE/USA-020

System name:

Employee Assistance Program (EAP) Counseling and Referral Records, Justice/USA-020

System location:

Records are maintained by the Executive Office for United States Attorneys (EOUSA) Employee Assistance Program (EAP) staff. Interested parties wishing to correspond regarding these records should direct their inquiries to the EAP Administrator, Executive Office for United States Attorneys, 600 E St. NW., Room 6800, Washington, DC 20530, (202) 514-1036.

Categories of individuals covered by the system:

Current and former employees of United States Attorneys Offices (USAOs) throughout the country and employees of the Executive Office for United States Attorneys (EOUSA) who have sought counseling or have been referred for counseling or treatment through the EAP. To a limited degree that counseling and referral may be provided to family members of these

employees, these individuals also are covered by the system. The remainder of this notice refers to all persons covered by the system as "EAP client(s)."

Categories of records in the system:

Records include any record, written or electronic, which may assist in referring, diagnosing, evaluating, counseling and/or follow-up with an EAP client, or resolving an EAP client's complaint or management's concerns (management consultation) regarding the EAP client's performance, attendance, or conduct problems. Included are the EAP counselor's intake, follow-up, and termination notes; pertinent psychosocial, medical, and employment history; relevant personnel documents; medical tests or screenings, including drug and alcohol tests and information on positive drug tests generated by the staff of the Drug Free Workplace Program or treatment facilities from which the EAP client may be receiving treatment; treatment and rehabilitation plans; and records of referrals. Referrals include those to community treatment resources and social service agencies that provide financial or other assistance which may or may not be related to mental health or general medical services. Where community referrals have been made, records may include relevant information related to counselor diagnosis, prognosis, treatment, and evaluation, together with follow-up information that may be generated by the community program providing the relevant services. Other records included in the system are the written consent forms used to permit the flow of information outside the EAP. Records may also include account information, such as contractor bills and government payments, when EAP services are provided by an EAP contractor.

Authority for maintenance of the system:

42 U.S.C. 290dd et seq.; 42 CFR part 2; 5 U.S.C. 3301, 7361, 7362, 7901 and 7904; 44 U.S.C. 3103; Executive Order 12564; and Pub. L. 100-71, sec. 503 (July 11, 1987).

Purpose(s):

Records are maintained to document the work performed by the EAP on behalf of the EAP client and to allow for the tracking of the EAP client's progress and the client's participation in the EAP or community programs. These records may also be used to track compliance with Abeyance or Last Chance agreements that include treatment options, in which the EAP is an integral part of establishing and/or monitoring treatment compliance as agreed by the EAP client and management.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

In addition to those disclosures permitted by the Privacy Act itself, 5 U.S.C. 552a(b), relevant information may be disclosed from this system of records without EAP client consent as follows: To the extent that the release of alcohol and drug abuse records is more restrictive than other records subject to the Privacy Act, EOUSA EAP staff will follow such restrictions. See 42 U.S.C. 290dd et seq.; 42 CFR part 2.

- a. To contractors that may provide EAP counseling and other services related to the administrative and financial management of the EAP program to the extent that it is appropriate, relevant, and necessary to enable the contractor to perform his or her court treatment, rehabilitation, and evaluation responsibilities.
- b. To appropriate state or local authorities to report, where required under state law, incidents of suspected child, elder or domestic abuse or neglect.
- c. To any person or entity to the extent necessary to prevent imminent threat of serious harm to client or others.
- d. When an individual to whom a record pertains has been determined to be mentally incompetent by a physician or under legal disability, to any person who is legally responsible for the care of the individual.
- e. To any person or entity to the extent necessary to meet a bona fide medical emergency.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Information in this system is maintained on paper and computer discs in accordance with 42 CFR 2.16.

Retrievability:

Records are indexed and retrieved by identifying number or symbol, cross-indexed to EAP.

client names.

Safeguards:

Paper records and computer discs are kept in locked GSA-approved security containers; the computer discs are password-protected. Only EOUSA EAP staff will have access to records. Records may be reviewed by any EAP staff member as may be needed to provide EAP services. No record may be released by the EAP staff without prior approval of the System Manager.

Retention and disposal:

Records are retained for three years after the EAP client ceases contact with the counselor, in accordance with General Records Schedule No. 1, Item No. 26) unless a longer retention period is necessary because of administrative or judicial proceedings. In such cases, the records are retained for six months after the conclusion of the legal proceedings. Paper records are destroyed by shredding, which must be performed by an EAP staff member. Computer discs are erased, degaussed, or physically destroyed by an EAP staff member.

System manager(s) and address:

The System Manager is the EAP Administrator, Executive Office for United States Attorneys, 600 E St. NW., Room 6800, Washington, DC 20530 (202) 514-1036.

Notification procedure:

Same as Record Access Procedures.

Record access procedures:

Make all requests for access in writing to the EAP System Manager identified above. Clearly mark the envelope and letter "Freedom of Information Act/Privacy Act Request." Provide name and notarized signature of the individual who is the subject of the record, the date during which the individual was in EAP counseling, any other information which may assist in identifying and locating the record, and a return address. Pursuant to 28 CFR 16.41(d), original signature on a "Certification of Identity" form (DOJ-361) may be submitted in lieu of notarized signature. This form may be obtained from the Department of Justice web site

<http://www.usdoj.gov>.

Contesting record procedures:

Direct all requests to contest or amend information to the EAP System Manager identified above. The request should follow the Record Access Procedures, listed above, and should state clearly and concisely the information being contested, the reason for contesting it, the proposed amendment thereof. Clearly mark the envelope and letter "Freedom of Information Act/Privacy Act Request."

Record source categories:

Records are generated by EAP personnel, referral counseling and treatment programs individuals, the EAP client who is the subject of the record, the personnel office, the EC Legal Counsel's Office, and the EAP client's supervisors. In the case of drug abuse counseling, records may also be generated by the staff of the Drug-Free Workplace Program and the Medical Review Officer.

Exemptions claimed for this system:

None.

[\[TOP\]](#)

JUSTICE/USA-999

System name:

Appendix of United States Attorneys' office locations: (Written requests for access to records of any of the following U.S. Attorneys' offices except the District of Columbia may be addressed to: FOIA/Privacy Unit, Patrick Henry Building, 601 D Street NW, room 6410, Washington 20530.

Requests for access to records in the District of Columbia may be addressed to: FOIA/Privacy Unit, United States Attorney's Office for the District of Columbia, Judiciary Center Building, 500 Constitution Avenue NW, Washington, DC 20001.)

Systems are located as listed below:

ALABAMA

Northern District

200 Federal Bldg., 1800 5th Ave. N., Birmingham 35203

Middle District

PO Box 197, Montgomery 36101

Southern District

169 Dauphin St., Suite 200, Mobile 36602

ALASKA

222 W. 7th Ave., No. 9, Federal Bldg. & Courthouse, Rm. C-253, Anchorage, 99513-75

*Rm. 310, New Federal Bldg. & Courthouse, 101 12th Ave., Box 2, Fairbanks 99701

ARIZONA

4000 U.S. Courthouse, 230 N. First Ave., Phoenix 85025

*Suite 8310, 110 South Church Ave., Tucson 85701

ARKANSAS

Eastern District

PO Box 1229, Little Rock 72203

Western District

PO Box 1524, Fort Smith 72902

CALIFORNIA

Northern District

450 Golden Gate Ave., Box 36055, San Francisco 94102

*280 South First St., Rm. 371, San Jose 95113

Eastern District

3305 Federal Bldg., 650 Capitol Mall, Sacramento 95814

*4304 Federal Bldg., 1130 O St., Fresno 93721

Central District

312 N. Spring St., Los Angeles 90012

*751 West Santa Ana Blvd., Santa Ana 92701

Southern District

5-N-19 U.S. Courthouse, 940 Front St., San Diego 92189

COLORADO

Suite 1200, Federal Bldg., Drawer 3615, 1961 Stout St., Denver 80294

CONNECTICUT

PO Box 1824, New Haven 06508

*250 Federal Bldg., 450 Main St., Hartford 06103

*309 Federal Building & Courthouse, 915 Lafayette Blvd., Bridgeport 06603

DELAWARE

Manufacturer's Hanover Plaza, 1201 Suite 1100, PO Box 2046, Wilmington 19899–2046

DISTRICT OF COLUMBIA

Judiciary Center Bldg. 555 4th St., NW, Washington, DC 20001 (Information)

Superior Court Division (Information)

FLORIDA

Northern District

315 S. Calhoun St., Suite 510, Tallahassee, 32301

*114 East Gregory St., Pensacola 32501

*401 SE 1st Ave., Room 318, Gainesville, 32602

Middle District

Rm. 400 Robert Timberlake Bldg., 500 Zack Street, Tampa 33602

*PO Box 600, Jacksonville 32201

*201 Federal Bldg., 80 N. Hughey Ave., Orlando 32801

*2000 Main St., The Barnett Centre, Suite 701,

Fort Myers, 33901

Southern District

155 South Miami Ave., Miami 33130

*Rm. 202B, 299 E. Broward Blvd., Fort Lauderdale 33301

*701 Clematis St., West Palm Beach 33401

*505 S. 2nd St., Suite 200, Ft. Pierce, 34950

GEORGIA

Northern District

Rm. 1800 Richard Russell Bldg., 75 Spring St. SW, Atlanta 30335

Middle District

PO Box U, Macon 31202

Southern District

PO Box 8999, Savannah 31412

*PO Box 2017, Augusta 30903—All mail goes to Savannah

GUAM

Suite 502–A, Pacific News Bldg., 238 Archbishop Flores St., Agana 96910

*3rd Floor, Horiguchi Bldg., PO Box 377, Saipan, MP 96950

HAWAII

Rm. 6100, PJKK Federal Bldg., Box 50183, 300 Ala Moana Blvd., Honolulu 96850

IDAHO

Rm. 328, Federal Bldg., Box 037, 550 W. Fort St., Boise 83724

ILLINOIS

Northern District

1500 South, Everett McKinley Dirksen Bldg., 219 S. Dearborn St., Chicago 60604

*211 South Court St., Rockford 61101

Southern District

9 Executive Dr., Suite 300, Fairview Heights, 62208

Central District

PO Box 375, Springfield 62705

*Rm. 253, Federal Building, 100 NE Monroe St., Peoria 61602

*14 Towne Centre, 2 East Main St., Danville 61832

*211 19th St., Room 14, Rock Island 61201

INDIANA

Northern District

1001 Main St., Suite A, Dyer 46311

*3128 Federal Bldg., 1300 S. Harrison St., Fort Wayne 46802

*MO-1 Federal Bldg., 204 S. Main St., South Bend 46601

Southern District

U.S. Courthouse, 5th Floor, 46 East Ohio St., Indianapolis 46204

IOWA

Northern District

425 2nd St., SE, Suite 950, The Center, Cedar Rapids 52401

*PO Box 3629, Sioux City 51102

Southern District

115 U.S. Courthouse, East 1st & Walnut Sts., Des Moines 50309

KANSAS

1200 Epic Center, 301 N. Main, Wichita 67202–4812

*444 Quincy St., Topeka 66683

*412 Federal Bldg., 812 N. Seventh St., Kansas City 66101

KENTUCKY

Eastern District

110 W. Vine St., Suite 400, Lexington 40507

*PO Box 72, Covington 41012

Western District

Bank of Louisville Bldg., 510 W. Broadway, 10th Floor, Louisville 40202

LOUISIANA

Eastern District

Hale Boggs Federal Bldg., Rm., 210, 501 Magazine St., New Orleans 70130

Middle District

339 Florida St., 6th Floor, Baton Route 70801

Western District

401 Edwards St., Suite 2100, Shreveport 71101–6133

*600 Jefferson St., Suite 1000, Lafayette 70501–7206

MAINE

East Tower, 6th Floor, 100 Middle St. Plaza, Portland 04101

99 Franklin St., Bangor 04401

MARYLAND

8th Floor, U.S. Courthouse, 101 W. Lombard St., Baltimore 21201

MASSACHUSETTS

1107 John W. McCormack Federal Bldg., USPO & Courthouse, Boston 02109

*1550 Main Street, Rm. 533, U.S. Courthouse, Springfield 01103

MICHIGAN

Eastern District

817 Federal Bldg., 231 W. Lafayette, Detroit 48226

*PO Box 26, 204 Federal Bldg., 1000 Washington St., Bay City 48707

*204 Federal Bldg., 600 Church St., Flint 48502

Western District

399 Federal Bldg., 110 Michigan St. NW, Gerald Ford Fed. Bldg., Grand Rapids 49503

*D&N Bank of Marquette Bldg., PO Box 20, Marquette 29855

MINNESOTA

234 U.S. Courthouse, 110 South 4th St., Minneapolis 55401

*678 U.S. Courthouse, 316 N. Robert St., St. Paul 55101

MISSISSIPPI

Northern District

PO Drawer 886, Oxford 38655

Southern District

188 East Capitol St., Rm. 500, Jackson 39201

*PO Box 1417, Biloxi 39533

MISSOURI

Eastern District

401 U.S. Court & Custom House, 1114 Market St., St. Louis 63101

*PO Box 2107, Cape Girardeau, 63702–2107

Western District

1201 Walnut, Suite 300, Kansas City 64106–2149

*Hammons Tower Suite 500, 901 St. Louis St., Springfield 65806–2511

MONTANA

PO Box 1478, Billings 59103

*167 Federal Bldg., 400 N. Main, Butte 59703

*PO Box 3447, Great Falls 59401

*Drawer 10031, Federal Bldg., 301 South Park Ave., Helena 59626

NEBRASKA

PO Box 1228, DTS, Omaha 68101–1228

*487 Federal Bldg., 100 Centennial Mall North, Lincoln 68508

NEVADA

Box 16030, Las Vegas 89101

*Rm. 2–032, 300 Booth St., Reno 89509

NEW HAMPSHIRE

55 Pleasant Street Rm. 439, PO Box 480, Concord 03302–0480

NEW JERSEY

Federal Bldg., 970 Broad St., Room 502, Newark 07102

*402 East State St., Rm. 502, Trenton 08608

*PO Bldg., 401 Market St., Fifth Floor, Camden 08101

NEW MEXICO

PO Box 607, Albuquerque 87103

*U.S. Courthouse, 200 East Griggs St., Rm. E-108, Las Cruces 88001

NEW YORK

Northern District

PO Box 7198, 100 South Clinton St., Syracuse 13261-7198

* U.S. Courthouse & Post Office, Room 231, 445 Broadway, Albany 12207

*319 Federal Bldg., Binghamton 13901

Eastern District

U.S. Courthouse, 225 Cadman Plaza East, Brooklyn 11201

*825 East Gate Blvd., Garden City 11530

*300 Rabro Drive, Hauppauge 11788

Western District

502 U.S. Courthouse, 68 Court St., Buffalo 14202

*233 U.S. Courthouse, 100 State St., Rochester 14614

Southern District

One St. Andrews Plaza, New York 10007

*150 Grand St., 4th Floor, White Plains, NY 10601

NORTH CAROLINA

Eastern District

310 New Bern Ave., Suite 800, Raleigh 27601–1461

Middle District

PO Box 1858, Greensboro 27402

Western District

Rm. 306, U.S. Courthouse, 100 Otis St., Asheville 28801–2611 (all mail goes to Charlotte)

*Rm. 260, U.S. Courthouse, 401 W. Trade St., Charlotte 28202

NORTH DAKOTA

PO Box 2505, Fargo 58108

*PO Box 699, Bismarck 58502

OHIO

Northern District

1800 Bank One Center, 600 Superior Ave. East, Cleveland 44114–2600

*208 Federal Bldg., 2 South Main St., Akron 44308

*307 U.S. Courthouse, 1716 Spielbusch Ave., Toledo 43624

Southern District

2 Nationwide Plaza, 280 N High St., 4th Floor, Columbus 43215

*5th & Walnut Sts., 220 U.S. Post Office & Courthouse, Cincinnati 45202

PO Box 280, Mid City Station, Dayton 45402

OKLAHOMA

Northern District

3900 U.S. Courthouse, 333 W. Fourth St., Tulsa 74103

Eastern District

333 Federal Courthouse, 5th & Okmulgee, Muskogee 74401

Western District

Rm. 4434, U.S. Courthouse & Federal Office Bldg., Oklahoma City 73102

OREGON

888 SW 5th Ave., Suite 1000, Portland 97204–2024

*701 High St., Eugene 97401

PENNSYLVANIA

Eastern District

3310 U.S. Courthouse, Independence Mall West, 601 Market St., Philadelphia 19106

Middle District

PO Box 309, Scranton 18501–0309 (send USA mail to Harrisburg)

*Suite 1162 Federal Bldg. 3rd & Walnut Sts., PO Box 11754 Harrisburg 17108

*Rm. 307, US Post Office Bldg., Lewisburg 17837

Western District

633 USPO & Courthouse, 7th Ave. & Grant St., Pittsburgh 15219

*Rm. 137, U.S. Courthouse & Federal Bldg., 617 State St., Erie 16501

*Suite 224, 10 Traffic Bldg., 319 Washington Ave., Johnstown, 15901

PUERTO RICO

Federal Office Bldg., Rm. 452, Carlos E. Chardon Ave., Hato Rey 00918

RHODE ISLAND

10 Dorrance St., 10th Floor, Providence 02903

SOUTH CAROLINA

1st Union Blvd., 1441 Main St., Suite 500, Columbia 29201

*PO Box 978, Charleston 29402

*PO Box 10067, Greenville 29603

*PO Box 1567, Florence 29503

SOUTH DAKOTA

PO Box 1073, Sioux Falls 57101

*PO Box 2893, Rapid City 57709

*326 Federal Bldg. & Courthouse, 225 S. Pierre St., Pierre 57501

*311 PO & Courthouse Bldg., 102 SE Fourth Ave., Aberdeen 57401

TENNESSEE

Eastern District

PO Box 872, Knoxville 37901

*1100 Market St., Suite 301, Chattanooga 37402

*104 1/2 W. Summer St., Greenville 37743

*208 Sunset Drive, Suite 509, Johnson City 37604

Middle District

110 9th Ave. S., Suite A961, Nashville 37203–3870

Western District

1026 Federal Office Bldg., 167 N. Main St., Memphis 38103

USPO & Courthouse Bldg., Rm. 308, 109 South Highland, Jackson 38302

TEXAS

Northern District

Burnett Plaza, Suite 1700, 801 Cherry St., Ft. Worth 76102–6897

*Rm. 16G28, U.S. Federal Bldg. & Courthouse, 1100 Commerce St., Dallas 75242

*Rm. C–201, U.S. Federal Bldg. & Courthouse, 1205 Texas Ave., Lubbock 79401

PO Box 13236, Amarillo 79101–1559

Southern District

PO Box 61129, Houston 77208

*PO Box 886, Laredo 78042–0886

*PO Box 1671, Brownsville 78522

*Wilson Plaza, Suite 1400, 606 N. Carancahua, Corpus Christi 78476

*Texas Commerce Bldg., 1701 West Highway 83, Suite 305, McAllen 78501–5159

Eastern District

350 Magnolia St., Suite 150, Beaumont 77701–2237

*110 N. College, Suite 600, Tyler 75702

*One Grand Centre, Suite 504, 1 Grand Ave., Sherman 75090

Western District

727 East Durango Blvd., Suite A–601, San Antonio 78206

*Rm. 353 U.S. Courthouse Bldg., 511 E. San Antonio Ave., El Paso 79901

*816 Congress Ave., Suite 650, First City Centre, Austin 78701

*U.S. Courthouse, 200 E. Wall St., Midland 79701

*700 University Parks Dr., Suite 770, Waco 76706

UTAH

U.S. Courthouse, Room 476, 350 South Main Street, Salt Lake City 84101

VERMONT

PO Box 570, Burlington 05402

*PO Box 10, Rutland 05701

VIRGIN ISLANDS

PO Box 1440, Charlotte Amalie, St. Thomas 00804–1440

All Mail to This Office

*1108 King St., Suite 201, Christiansted, St. Croix 00820–4951

VIRGINIA

Eastern District

1101 King Street, Suite 502, Alexandria 22314

*Main Street Center, Suite 1800, 600 E. Main St., Richmond 23219

*World Trade Center, Suite 1800, 101 W Main St., Norfolk 23510

Western District

*PO Box 1709, Roanoke 24008

*PO Box 1098, Abingdon 24210

WASHINGTON

Eastern District

PO Box 1494, Spokane 99210–1494

*PO Box 1363, Yakima 98907–1363

Western District

3600 Seafirst 5th Ave. Plaza, 800 5th Ave., Seattle 98104

*Suite 400, 1201 Pacific Ave., Tacoma 98402

WEST VIRGINIA

Northern District

PO Box 591, Wheeling 26003

*PO Box 190, Elkins 26241

*PO Box 750, Clarksburg 26302

*U.S. Courthouse, Room 236, Martinsburg 25401

Southern District

PO Box 3234, Charleston 25332

*PO Box 1239, Huntington 25714

*Branch Office

WISCONSIN

Eastern District

330 Federal Bldg., 517 E. Wisconsin Ave., Milwaukee 53202

Western District

600 West Washington Ave., PO Box 1585, Suite 200, Madison 53703

WYOMING

PO Box 668, Cheyenne 82003

NORTH MARIANNA ISLANDS

c/o U.S. Attorney's Office, 6th Floor, Naura Bldg., PO Box 377, Saipan, CM 96950

[\[TOP\]](#)

United States Marshall Service

JUSTICE/USM-001

System name:

U.S. Marshals Service Badge & Credentials File.

Security classification:

Limited official use.

System location:

Human Resources Division, United States Marshals Service, CS-3, Washington, DC 20530-1000.

Categories of individuals covered by the system:

Current and former U.S. Marshals Service (USMS) personnel, other federal employees, student volunteers or other workers when they are performing work for the USMS.

Categories of records in the system:

Personnel data system established to control issuance of badges and credentials to US personnel which contains photographs of all employees and hand receipts showing the employee's name, title, duty location, badge and credential numbers, and date of issue

Authority for maintenance of the system:

5 U.S.C. 301 and 44 U.S.C. 3101.

Purpose(s):

The Badge & Credentials File system assists in controlling the issuance of badges and credentials to USMS personnel which are used for identification purposes in the perform of official duties.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

This file serves as a record of issuance of credentials. Information from this file may be disclosed:

(a) To any criminal, civil, or regulatory law enforcement authority (whether federal, state territorial, local, tribal, or foreign) where the information is relevant to the recipient entity enforcement responsibilities;

(b) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(c) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government when necessary to accomplish an agency function related to this system or its records;

(d) To the news media and the public, including disclosures pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(e) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the

subject of the record;

(f) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(g) To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings;

(h) Where a record, either alone or in conjunction with other information, indicates a violent potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, territorial, local, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(i) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

(j) To a former employee of the Department for purposes of: responding to an official inquiry from a federal, state, territorial, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes of the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(k) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft, fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:***STORAGE:***

Records are kept in standard folders and kept electronically.

RETRIEVABILITY:

Records are indexed and retrieved by the individual's name and numerical order of badge credentials.

Safeguards:

Access is restricted to personnel of the Background and Suitability Team, Human Resources Division. Records are maintained in metal filing cabinets which are locked during non-duty hours.

RETENTION AND DISPOSAL:

Records are kept for duration of employee's tenure in the service. Records are destroyed, superseded or obsolete.

SYSTEM MANAGER(s) and address:

Assistant Director, Human Resources Division, United States Marshals Service, CS-3, Washington, DC 20530-1000.

Notification procedure:

Same as "Record access procedures."

Record access procedures:

A request for access to a record from this system shall be made in writing with the envelope and the letter clearly marked "Privacy Act Request." It should clearly indicate the name of the requester, the nature of the record sought and the approximate dates covered by the request. The requester shall also provide the required verification of identity (28 CFR 16.41(d)) and provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above, Attention: FOI/PA Officer.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the address of the System Manager listed above, Attention: FOI/PA Officer, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Record of Notification of Employment by U.S. Marshals Service, Human Resources Division, and the individuals for whom the badges/credentials are made.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

JUSTICE/USM-002

System name:

Internal Affairs System.

Security classification:

Limited Official Use.

System location:

United States Marshals Service (USMS), Operations Support Division, CS-3, Washington, DC 20530-1000.

Categories of individuals covered by the system:

USMS employees reported for or investigated for alleged misconduct.

Categories of records in the system:

The Internal Affairs System contains statements of the investigator and witnesses, exhibit reports of investigations prepared by the Office of Inspection, USMS, on findings of alleged misconduct of USMS employees, and records on the disposition of the investigation.

Authority for maintenance of the system:

28 U.S.C. 509 and 510; 5 U.S.C. 301; 44 U.S.C. 3101; and 28 CFR 0.111(n).

Purpose(s):

The Internal Affairs system is maintained in order to carry out the responsibility of investigating allegations of improper conduct on the part of USMS employees, and to support adverse personnel actions and proceedings which may result based on the findings of the investigation.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records or information may be disclosed:

(a) To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation case arising from the matters of which they complained and/or of which they were a victim.

(b) Where a record, either alone or in conjunction with other information, indicates a potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

- (c) To any person or entity that the USMS Office of Internal Investigations has reason to believe possesses information regarding a matter within the jurisdiction of the USMS Office of Internal Investigations, to the extent deemed to be necessary by the Office in order to elicit such information or cooperation from the recipient for use in the performance of an authorized activity;
- (d) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;
- (e) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit;
- (f) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body, when the adjudicator determines the records to be relevant to the proceeding;
- (g) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;
- (h) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;
- (i) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;
- (j) To a former employee of the Department for purposes of: responding to an official inquiry from a federal, state, territorial or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with

former employee that may be necessary for personnel-related or other official purposes the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(k) To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings.

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or confirmed that the security or confidentiality of information in the system of records has compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Originals stored in standard file folders. Duplicate copies are maintained on compact disc.

Retrievability:

Information is retrieved by the employee's name and case file number.

Safeguards:

Records are stored in locked safe. Access to automated records is protected by user identification and passwords.

Retention and disposal:

Records are transferred to the Washington National Records Center three years after the case or investigation is closed, and destroyed 10 years after the close of the case or investigation.

System manager(s) and address:

Chief, Office of Inspection, Operations Support Division, U.S. Marshals Service, CS-3, Washington DC 20530-1000.

Notification procedure:

Same as the "Records access procedures."

Record access procedures:

To the extent that this system is not subject to exemption, it is subject to access and declassification determination as to exemption shall be made at the time a request for access is received. A request for access to a record from this system shall be made in writing, with the envelope clearly marked "Privacy Act Request." It should clearly indicate name of the requester, the nature of the record sought and approximate dates covered by the record. The requester shall also provide the required verification of identity (28 CFR 16.41(d)) and a return address for transmitting the information. Access requests will be directed to the System Manager listed above, Attention: FOI/PA Officer.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager identified above, stating clearly and concisely what information is being contested, the reason for contesting it, and the proposed amendment to the information sought.

Record source categories:

Sources of information contained in this system are the individuals covered by the system, individuals and entities contacted by investigators, and government records.

Exemptions claimed for the system:

The Attorney General has exempted this system from subsections (c)(3) and (4)(d), (e)(3), (e)(4)(G) and (H), (e)(5), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552 and (k)(5). To the extent that investigations reveal actual or potential criminal or civil violations, this system is additionally exempt from subsection (e)(8) of the Privacy Act pursuant to 5 U.S.C. 552(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and have been published in the *Federal Register*. See 28 CFR 16.101.

[\[TOP\]](#)

JUSTICE/USM-004

System name:

Special Deputation Files.

Security Classification:

Limited Official Use.

System location:

United States Marshals Service (USMS), Investigative Services Division, CS-4, Washington, DC 20530-1000.

Categories of individuals covered by the system:

Federal, state and local law enforcement employees; physical security and personal protection employees; USMS employees; and USMS contract personnel appointed to perform the functions of Deputy U.S. Marshals.

Categories of records in the system:

Special Deputation files contain agency request letters, individual applications for special deputation, notifications to local U.S. Marshal to swear in special deputies, copies of oaths.

office and credentials of persons utilized as deputy marshals.

Authority for maintenance of the system:

28 CFR subpart T, 0.112, 28 U.S.C. 562.

Purpose(s):

The USMS is authorized to deputize selected persons to perform the functions of a Deputy U.S. Marshal whenever the law enforcement needs of the USMS so require, to provide courtroom security for the Federal judiciary, and as designated by the Associate Attorney General pursuant to 28 CFR 0.19(a)(3). USMS Special Deputation files serve as a central record of the special deputations granted by the USMS to assist in tracking, controlling and monitoring the Special Deputation Program. Routine uses of records maintained in the system include the following categories of users and the purposes of such uses: Records or information may be disclosed:

- (a) To a federal, state or local law enforcement agency regarding that agency's USMS deputized employees;
- (b) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;
- (c) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;
- (d) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;
- (e) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(f) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(g) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(h) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings;

(i) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit;

(j) A record may be disclosed to designated officers and employees of state, territorial, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prison detainees, to the extent that the information is relevant and necessary to the recipient agency's decision;

(k) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has

compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (w maintained by the Department or another agency or entity) that rely upon the compromi information; and (3) the disclosure made to such agencies, entities, and persons is reas necessary to assist in connection with the Department's efforts to respond to the suspec confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

Policies and practices for storing, retrieving, accessing, retaining and disposing of records in the system:

Storage:

Records are filed in standard file cabinets. Duplicate copies of paper records are stored on magnetic discs.

Retrievability:

Files are indexed by name and by government department.

Safeguards:

Records are kept in a locked file. Computerized records are password protected.

Retention and disposal:

Records are cut off annually upon expiration and destroyed when they are five years old.

System manager(s) and address:

Chief of Special Deputation Unit, Investigative Services Division, U.S. Marshals Service, Washington, DC 20530-1000.

Notification procedures:

Same as the "Records access procedures."

Records access procedures:

A request for access to a record from this system shall be made in writing, with the envelope and the letter clearly, marked "Privacy Act Request." It should clearly indicate name of the requester, the nature of the record sought and approximate dates covered by the record. The requester shall also provide the required verification of identity (28 CFR 16.41(d)) and provide a return address for transmitting the information. Access requests will be directed to the System Manager listed above, Attention: FOI/PA Officer.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager identified above, stating clearly and concisely what information is being contested, the reasons for contesting it and the proposed amendment to the information sought.

Record source categories:

Information is derived from individual applicants and agencies requesting special deputization.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

JUSTICE/USM-005***System name:***

U.S. Marshals Service Prisoner Processing and Population Management/Prisoner Track System (PPM/PTS).

Security classification:

Limited Official Use.

System location:

Primary System: Witness Security and Prisoner Operations, U.S. Marshals Service, 11th CS-4, Washington, DC 20530-1000.

Decentralized Segments: Each district office of the U.S. Marshals Service (USMS) maintains files on prisoners taken into custody of the U.S. Marshal for the respective district. addresses of USMS district offices are on the Internet at (<http://www.usmarshals.gov>

Centralized Segment: The Contractor with whom the USMS has contracted to establish and manage a nationwide integrated health care delivery system and to process and pay medical claims will maintain a single site for appropriate paper documents (e.g., invoices) and automated files online related to these activities (e.g., names and addresses of hospital physicians and other health care providers and support service systems).

Medical Records: Records generated by community physicians, hospitals, and ancillary support service systems developed by the Contractor as participants in the Preferred Provider Network (PPN) to deliver health care services for USMS prisoners are maintained by the respective offices of these licensed providers. Addresses of these licensed providers may be obtained by contacting the USMS Office of Interagency Medical Services (OIMS), Prisoner Services Division at the address above.

Categories of individuals covered by the system:

Arrestees, fugitives, prisoners, and other individuals under custody of the USMS and health care services providers under the USMS Managed Health Care Contract.

Categories of records in the system:

Any and all information necessary to complete administrative processes, safekeeping, health care, and disposition of individual Federal prisoners who are in custody pending criminal proceedings, together with any law enforcement related records generated during such

custody. Records include a compilation of basic information on each individual taken into U.S. Marshals Service's custody including identifying data, reason for U.S. Marshal custody (e.g., Federal indictment, complaint, or writ), the court disposition of charges, custody details and institutions to which individuals are committed or housed. The records also encompass Form USM-129, Prisoner Custody, Detention and Disposition Record (formerly DJ-100) prisoner photograph; personal history statement; fingerprint card; identification record; court notice; speedy trial notice; prisoner remand or order to deliver prisoner, and receipt for release of prisoner; property receipt; court records including writs, bail/bond release information, judgment and commitment and other court orders; prisoner alert notice; prisoner complaint; serious incident reports (and related investigatory information) filed by either the prisoner or officials or by other individuals at the institution where the prisoner is housed and covering a wide range of potentially serious issues, e.g., medical treatment of prisoners, and attempted escapes or alleged prisoner misconduct or criminal activity; designation requests to Bureau of Prisons (BOP) and BOP responses; information identifiable to informants, protected witnesses and confidential sources; access codes and data entry codes and message routing systems used to communicate with law enforcement officials regarding the custody and safekeeping of prisoners; and prisoner transportation requests to the Prisoner Transportation Division (and related records) which may include sensitive security data. Medical records included in the system consist of nurses' notes of medical problems, diagnosis, treatment recommendations, names of health care providers at the housing unit, social workers, attorneys, family members and USMS contact personnel; special issue or treatment notices; names and addresses of community treatment facilities, physicians and other community health care providers and support service systems, dates of service, provider tax identification numbers; medical conditions given, cost of care, and billing records. Medical records generated by health care providers may be included in this system of records, as necessary for continuity of care/appropriate or infectious disease control.

Authority for maintenance of the system:

18 U.S.C. 3149, 3193, 3604, 3621, 4002, 4006, 4086, 4285; 28 U.S.C. 509, 510, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000.

Purpose(s):

The Prisoner Processing and Population Management/Prisoner Tracking System (PPM/PT) is maintained to cover law enforcement and security related records which are generated at local USMS district offices in connection with the processing, safekeeping, and disposition of prisoners.

individuals in USMS's custody. Medical records included in this system assist consultation and coordination between the USMS district office, the housing unit, treatment facility, health care provider, transportation facility, and other Federal agencies, e.g., BOP, to ensure that prisoners in custody of the U.S. Marshals are given proper treatment. Through USMS nursing staff, districts are assisted in determining medical treatment necessary while the prisoner is in custody of the U.S. Marshal and in ensuring the prisoner's medical clearance for travel.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records or information may be disclosed:

(a) To other federal, state, local or foreign law enforcement agencies; contractors and/or subcontractors; contract detention or medical facilities; and health care providers to provide and ensure the safety and/or health of prisoners, the public, and law enforcement officials; to ensure fair and proper treatment of prisoners during custody and transfer of custody; to assist the USMS in pursuing any necessary inquiry/investigation of complaints, alleged misconduct or criminal activity; to process and pay medical claims; and to perform evaluation duties. For example, relevant records or information may be disclosed to secure the safe and efficient transfer of prisoners to other jurisdictions, to court appearances, or to the designated facility for service of sentence; to ensure that appropriate credit for time in custody is given; that appropriate medical treatment is provided; that all rights of the prisoner, whether statutory or humanitarian, or otherwise, are provided and protected; and to elicit information from which to initiate an inquiry/investigation and/or respond to prisoner complaints and reports of alleged misconduct or criminal activity; or, conversely, to enable those entities to respond to, or provide information relating to, such prisoner complaints or reports of misconduct or criminal activity.

(b) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, local, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

(c) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(d) To an actual or potential party to litigation or the party's authorized representative for

purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings;

(e) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(f) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(g) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(h) To federal, state, territorial, local, tribal, foreign or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit;

(i) A record may be disclosed to designated officers and employees of state, territorial, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient's decision;

(j) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(k) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, territorial, or local government entity or professional licensing authority in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee.

regarding a matter within that person's former area of responsibility;

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or confirmed that the security or confidentiality of information in the system of records has compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (w maintained by the Department or another agency or entity) that rely upon the compromi information; and (3) the disclosure made to such agencies, entities, and persons is reas necessary to assist in connection with the Department's efforts to respond to the suspec confirmed compromise and prevent, minimize, or remedy such harm.

Policies and procedures for storing, retrieving, accessing, retaining, and disposing records in the system:

Storage:

Information is stored in standard file cabinets. Duplicate copies of certain paper and ele records are stored on magnetic discs.

Retrievability:

Information is retrieved by name and/or number of individual in custody, and/or health c provider. Records retrieved by name or number of health care provider will consist of the provider's address, name and number of prisoners treated, claim number, dates of serv nature of service, amount billed, USMS amount allowed, amount saved, and percentage saved.

Safeguards:

Paper records are stored in locked files. Access to computerized data is restricted throu identification and discrete password functions. In addition, USMS district and headquar offices are secured behind locked doors around the clock and access is restricted to US personnel with official identification.

All USMS contractors must have personnel security clearances commensurate with the level of information processed by the system, in this case Limited Official Use. Encrypti

technology shall be applied to passwords and symmetric or private asymmetric keys, access by a system administrator or for system maintenance, and information stored on laptop computers. All information technology systems within a component are subject to the certification and accreditation process.

Retention and disposal:

General prisoner records are kept in active files until a prisoner has been transferred from custody of USMS. After a prisoner leaves USMS custody, the file is closed, and at the end of the year, closed files are separated from active files. Closed files are maintained for one year after separation, then are transferred to a Federal Records Center, and are destroyed after 10 years, or sooner, if ordered by the Court. This does not apply to records maintained by the Contractor, which are discussed below.

The Contractor will maintain all appropriate paper documents (i.e., invoices, etc.) and automated online files for the duration of the contract performance. Computer storage not containing Limited Official Use information will be overwritten or degaussed prior to release of the storage media outside the USMS. At the end of the contract, the contractor shall turn over all paper documents and automated files of the database offline to the USMS within two weeks of contract expiration. All paper documents and automated files of the database will be maintained in accordance with the General Records Schedule 6, Item 1a (Accountable Financial Files), as published by NARA, unless a longer retention period is necessary because of pending administrative or judicial proceedings.

The retention and disposal procedures for this system of records are in accordance with NARA disposition authority for the USMS which is NI 527-99-1, or the General Records Schedule as appropriate.

System manager(s) and address:

Assistant Director, Witness Security and Prisoner Operations, United States Marshals Service
11th Floor, CS-4, Washington, DC 20530-1000.

Notification procedure:

Same as "Record access procedures."

Record access procedures:

Requests for access must be in writing and should be addressed to the System Manager named above, Attention: FOI/PA Officer. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the information sought and must include the requester's full name, current address, and date and place of birth. The request must be signed, dated, and either notarized or submitted under penalty of perjury. Some information may be exempt from access provisions as described in the section entitled "Exemptions Claimed for the System." An individual who is the subject of a record in this system may access those records that are not exempt from disclosure. A determination whether a record may be accessed will be made at the time a request is received.

Contesting record procedures:

Individuals desiring to contest or amend information maintained in the system should direct their request to the system manager listed above, Attention: FOI/PA Officer, stating clearly and concisely the identifying information required above in "Record access procedures", what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. Some information may be exempt from contesting record procedures as described in the section entitled "Exemptions Claimed for the System." An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

Record source categories:

Information is received from the individual in custody; the courts, federal, state, territorial, tribal and foreign law enforcement agencies and personnel; witnesses; and medical care professionals and/or facilities.

Exemptions claimed for the system:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(3), (e)(5) and (e)(8) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register*. The rules are codified at 28 CFR 16.101(c)(r).

[\[TOP\]](#)

JUSTICE/USM-006

System name:

United States Marshals Service Training Files.

Security classification:

Limited official use.

System location:

a. Primary system: Human Resources Division, United States Marshals Service, CS-3, Washington, DC 20530-1000.

b. Decentralized segments: Individual training files and the Fitness in Total (FIT) Program training assessment files, identified as items (1) and (3) under "Categories of Records in the System," are located also at the USMS Training Academy, Department of Justice, Building 10, Glynnco, Georgia 31524. Each district office of the USMS maintains FIT files only on their respective participants in the FIT Program. The addresses of USMS district offices are on the Internet at <http://www.usdoj.gov/marshals/usmsofc.aspx>.

Categories of individuals covered by the system:

Trainees hired as Deputy U.S. Marshals and Deputy U.S. Marshals.

Categories of records in the system:

(1) Individual training files contain information on the individual's educational background, employee training history, and an individual career development plan; (2) skills files identify languages and other special skills possessed by the individual USMS employee; and (3) individual FIT Program training assessment files contain records on physical and medical examinations, blood tests, health histories, physical assessments, and administrative records on participation, goal setting and progress while in the program. The Certificate of Medical Examination (SF-78) is maintained in the primary system at USMS headquarters only.

obtained and placed in the district file by the individual FIT participant.

Authority for maintenance of the system:

28 U.S.C. 509, 510, and 569; 5 U.S.C. 301; 44 U.S.C. 3101; and 28 CFR 0.111(h).

Purpose(s):

Individual training files are used to make employment, promotion, or retention determinations for all Deputy U.S. Marshals; to develop training histories; and to determine training and promotion eligibility. In addition, FIT Program training assessment files are used to make hiring/retention determinations for Deputy U.S. Marshal personnel entering on duty as of 1, 1984 and later; to determine employees' eligibility to participate in the program; to tailor individual fitness program for each employee; to chart employee progress in the program; to determine the need for and to chart progress toward weight reduction; to develop physical fitness standards for performance appraisal purposes; and to examine statistically the physical fitness level of the USMS workforce against law enforcement populations and the general population of the United States. Skills files are used to identify special skills and language abilities possessed by personnel to aid in staffing special assignments which require such skills.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records or information may be disclosed as a routine use:

- (a) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;
- (b) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;
- (c) To appropriate officials and employees of a federal agency or entity which requires

information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit;

(d) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(e) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(f) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(g) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings;

(h) A record may be disclosed to designated officers and employees of state, territorial, (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prison detainees, to the extent that the information is relevant and necessary to the recipient agency's decision;

(i) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities;

(j) To a former employee of the Department for purposes of: responding to an official inquiry from a federal, state, territorial, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes.

where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(k) To appropriate agencies, entities, and persons when (1) the Department suspects or confirmed that the security or confidentiality of information in the system of records has compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Originals of paper records contained in this system are kept in standard file cabinets. Summary files, summaries of FIT Program training assessment records, and duplicates of paper records are stored on magnetic discs.

Retrievability:

Records are retrieved by the employee's name.

Safeguards:

Records are maintained in metal filing cabinets which are locked during non-duty hours. Access to headquarters is restricted by 24-hour guard service to employees with official and employee identification. Entry to the Training Academy and district offices is restricted generally to trainees/employees with official identification. Access to computerized records in this system is restricted to the responsible headquarters employees by assigned code.

Retention and disposal:

Files are maintained for five (5) years then the magnetic disks are erased and paper records are archived in the Federal Records Center and destroyed when 20 years old, unless the employee leaves the USMS at which time paper records are transferred to another agency and sent to the OPM records center.

System manager(s) and address:

Assistant Director, Human Resources Division, USMS, CS-3, Washington, DC 20530-1

Notification procedure:

Same as "Record access procedures."

Record access procedures:

Make all requests for access in writing and clearly mark letter and envelope "Freedom of Information Act/Privacy Act Request." Clearly indicate name of the requester, nature of the record sought, approximate dates of the records, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above, Attention: FOI/PA Officer, and provide a return address for transmitting the information.

Contesting record procedures:

Direct all requests to contest or amend information to the system manager listed above. Clearly and concisely the information being contested, the reasons for contesting it, and proposed amendment to the information sought. Clearly mark the letter and envelope "Freedom of Information Act/Privacy Act Request."

Record source categories:

Information contained in this system is collected from the individual, training personnel, Combined Federal Law Enforcement Training Academy, examining physicians, fitness coordinators, and personnel records.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

JUSTICE/USM-007

System name:

Warrant Information Network (WIN).

Security classification:

Limited Official Use.

System location:

Primary System: Investigative Services Division, U.S. Marshals Service (USMS), CS-4, Washington, DC 20530-1000.

Decentralized Segments: Each district office of the USMS maintains their own files. The addresses of USMS district offices are available on the Internet at <http://www.usdoj.gov/marshals/usmsofc.aspx>.

Categories of individuals covered by the system:

Individuals for whom federal warrants have been issued; individuals for whom State or local warrants have been issued when the warrant is part of a USMS sponsored multi-agency task force; individuals suspected in a state's case that has been adopted by a USMS-sponsored task force; individuals for whom the USMS is conducting a criminal investigation or aiding in a criminal investigation by another law enforcement agency; missing persons, including children for whom the USMS is conducting an investigation or aiding in a criminal investigation by another law enforcement agency; individuals, and their associates, who are the subject of an investigation or who may provide information, assistance or leads in USMS fugitive, criminal, or missing persons investigations.

Categories of records in the system:

Computerized records in this system consist of information pertaining to a warrant such as dates, issuing federal district, nature of the offense, investigative notes, information relating to subjects, including biographical data, physical description, and criminal history, and a subject's association with other individuals, dangerous gangs, extremist groups, or other organizations. The system also contains information concerning criminal and/or missing persons investigations, such as the evidence collected in support of criminal and/or missing persons investigations, the nature of the investigative reports, investigative notes, biographical data relating to the investigation's subject and the subject's associates. Information on associates includes physical description, photographs, numerical identifiers, addresses, driver's license information and investigative information furnished by other federal, state or local law enforcement or other government agencies and non-government sources. In addition to the abbreviated data described above, the complete file contains the warrant and other court records and internal correspondence relating to the warrant; photographs; wanted flyers/posters; and investigative reports relating to patterns of activity, leads, witnesses' and other persons' statements. Investigative reports include criminal record information from other federal, state, local, and foreign law enforcement agencies participating in or cooperating with USMS fugitive, criminal, or missing person investigations and apprehension efforts are also included in this system.

Authority for maintenance of the system:

28 U.S.C. 509, 510, and 561 *et seq.*; 28 CFR 0.111(a) and (q).

Purpose(s):

The USMS is responsible for ensuring the judicial system's effective operation through the execution of federal arrest warrants, parole violator warrants, federal custodial and extradition warrants, and by investigating fugitive, criminal, and missing person matters. The WIN system facilitates the efficient management and administration of warrant executions and USMS investigations of fugitive, criminal and missing person investigations through the collection, flow, analysis, dissemination and maintenance of records and information necessary to accomplish the system's missions.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records or information may be disclosed:

- (a) To public and private organizations, individuals, and federal, state, territorial, local and foreign agencies to the extent necessary to obtain information or cooperation in USMS investigations and apprehension efforts;
- (b) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, local, tribal, or foreign) where the information is relevant to the recipient entity enforcement responsibilities;
- (c) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or records;
- (d) In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;
- (e) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;
- (f) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;
- (g) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;
- (h) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings;
- (i) To federal, state, territorial, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit;

(j) A record may be disclosed to designated officers and employees of state, territorial, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prison detainees, to the extent that the information is relevant and necessary to the recipient agency's decision;

(k) To a former employee of the Department for purposes of: Responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft, fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to Consumer Reporting Agencies: Not Applicable.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are stored in standard file folders. Duplicate copies of paper records are stored on magnetic discs.

Retrievability:

Records are retrieved by individual names or identifying numbers.

Safeguards:

Except as otherwise noted in paragraph (b) under "Routine uses," access is restricted to personnel in the Investigative Services Division and in each USMS district office. Access to computerized records is safeguarded by user identification and password restrictions. Paper records are maintained in filing cabinets within supervised areas of the U.S. Marshals' Office. District and headquarters offices are locked during working and non-duty hours and entry is restricted to employees with official identification.

Retention and disposal:

Records are kept in an operating file until warrant is executed and then transferred to a closed file. Closed files are retained for one year after file is closed, then transferred to the Federal Records Center and destroyed after 55 years. Computerized records are retained indefinitely as an operating file or as a closed case file.

System manager(s) and address:

Assistant Director, Investigative Services Division, U.S. Marshals Service, CS-4, Washington, DC 20530-1000.

Notification procedure:

Same as "Record access procedures."

Record access procedures:

Make all requests for access in writing and clearly mark the letter and envelope "Freedom of Information/Privacy Act Request." Clearly indicate the name of the requester, nature of the record sought, approximate date of the record, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above, Attention: FOI/PA Officer, and provide a return address for transmitting the information.

Contesting record procedures:

Direct all requests to contest or amend information to the system manager identified above. State clearly and concisely the information being contested, the reason for contesting it, and the proposed amendment to the information sought. Clearly mark the envelope "Freedom of Information/Privacy Act Request."

Record source categories:

Information is obtained from the courts, federal, state, local and foreign law enforcement agencies, public and private organizations, commercial information resellers, witnesses, informants, and other persons interviewed during the course of the fugitive, criminal, or person investigations.

Exemptions claimed for the system:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(1) and (3), (e)(4)(G) and (H), (e)(5), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and have been published in the *Federal Register*. See 28 CFR 16.11

[\[TOP\]](#)

JUSTICE/USMS-008

System name:

Witness Security Files Information System.

Security classification:

Limited Official Use.

System location:

Witness Security and Prisoner Operations, United States Marshals Service (USMS), CS
Washington, DC 20530-1000.

Categories of individuals covered by the system:

Government witnesses or potential witnesses and their families authorized to participate in the Witness Security Program.

Categories of records in the system:

This system contains requests to enter the Witness Security Program, authorizations to enter the program, identifying and background information on the witness and/or the witness' family, funding information, and moving information.

Authority for maintenance of the system:

28 U.S.C. 509, 510, 524, and 561 et seq.; 5 U.S.C. 301; 44 U.S.C. 3101; 28 CFR 0.111 (28 CFR 0.111); 5 U.S.C. 3521.

Purpose(s):

The USMS provides for the security, health and safety of government witnesses and their immediate dependants whose lives are in danger as a result of their testimony against organized crime, drug traffickers, terrorists and other major criminals. The Witness Security Files are used to plan and accomplish the major functions involved in the protection of government witnesses and their families.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records or information may be disclosed as follows:

- (a) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;
- (b) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;
- (c) To the National Archives and Records Administration for purposes of records management.

inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(d) Where a record, either alone or in conjunction with other information, indicates a potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, territorial, local, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(e) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings;

(f) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit;

(g) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(h) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(i) To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, local, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities;

(j) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has

compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (w maintained by the Department or another agency or entity) that rely upon the compromi information; and (3) the disclosure made to such agencies, entities, and persons is reas necessary to assist in connection with the Department's efforts to respond to the suspec confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

Records in this system are not appropriate for disclosure to consumer reporting agencie

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Records are kept in file folders and in a computerized database.

Retrievability:

Filed and retrieved by special ID number.

Safeguards:

Access is restricted to Witness Security personnel using locks and alarm devices, passw and/or encrypting data communications. The records are located in a restricted area of Headquarters under 24-hour guard protection with entry controlled by official and electr identification.

Retention and disposal:

Witness case files will be closed upon witness termination from the Witness Security Pr and retained in the custody of the USMS for 15 years, thereafter they will be transferred Federal Records Center and destroyed 75 years after termination. Financial records are destroyed after three years and three months in accordance with General Records Sche 6, 7 and 8.

System manager(s) and address:

Witness Security and Prisoner Operations, U.S. Marshals Service, CS-4, Washington, DC 20530-1000.

Notification procedure:

Same as the "Record access procedures."

Record access procedures:

Make all requests for access in writing and clearly mark letter and envelope "Privacy Act Request." Clearly indicate name of the requester, nature of the record sought, approximate dates of the record, and provide the required verification of identity (28 CFR 16.41(d)). Direct requests to the system manager identified above, Attention: FOI/PA Officer, and provide return address for transmitting the information.

Contesting record procedures:

Direct all requests to contest or amend information to the system manager listed above. Clearly and concisely state the information being contested, the reasons for contesting it, and proposed amendment to the information sought. Clearly mark the letter and envelope "Privacy Act Request."

Record source categories:

Information is provided by the witnesses and their families, the court, federal, state, territorial, local, tribal and foreign law enforcement agencies, and medical personnel.

Exemptions claimed for the system:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e)(3), (e)(4)(G) and (H), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (e) and have been published in the *Federal Register*. See 28 CFR 16.101.

[\[TOP\]](#)

JUSTICE/USM-009

System name:

Inappropriate Communications/Threat Information System.

Security classification:

Limited Official Use.

System location:

Primary System: Investigative Services Division, U.S. Marshals Service (USMS), CS-4, Washington, DC 20530-1000.

Decentralized Segments: Each district office of the USMS maintains their own files. The addresses of USMS district offices are available on the Internet at <http://www.usdoj.gov/marshals/usmsofc.aspx>.

Categories of individuals covered by the system:

Individuals who have inappropriately communicated with, directly threatened, or pose a threat to USMS protectees, including federal judges, prosecutors, and other court officials. U.S. Marshals, deputies and other law enforcement officers, courtroom security, and federal property and buildings; associates of the threat or inappropriate communication initiator; individuals reported by state or local agencies to the USMS who have threatened to harm or local judicial officials.

Categories of records in the system:

Manual and automated records which consist of information related to the inappropriate communication or threat, including type of communication, the means by which it was made, and information contained in the communication such as dates, locations, and events; a copy of the communication or threat and other internal USMS correspondence relating to the communication; biographical data including physical description, photograph, and criminal history information—in particular, known history of violence and skills related to the nature of the threat; investigative information including associations with other individuals and data

gangs, extremist groups, or other organizations; information on associates including physical descriptions, photographs, numerical identifiers, addresses, driver's license information; investigative information furnished by other federal, state, territorial, tribal, and local law enforcement or other government agencies and non-government sources.

Authority for maintenance of the system:

28 U.S.C. 509, 510, and 561 *et seq.*; 5 U.S.C. 301; 44 U.S.C. 3101; and 28 CFR 111(c)(f).

Purpose(s):

The USMS is required to protect government witnesses, U.S. Attorneys and their assistants; federal jurists and other court officers; to provide for courtroom security; and to assist in protecting federal property and buildings. The USMS also conducts Federal law enforcement activities itself, *e.g.*, warrant apprehension investigations, which subject its officers to some danger. These operations require acquiring information to allow an accurate assessment of the existence and extent of the dangers posed, including specific threats, to aid in responding to specific security assignments and needs, as well as developing protective measures in advance. With the information collected, officials determine and carry out operating plans, funding, personnel, and any special resources needed to counteract threat situations.

Individuals reported by State and local agencies to the USMS who have threatened to harm state or local judicial officials often appear before the federal bar as a result of appeals, habeas rights suits, continuing criminal behavior, etc. Such individuals may continue their inappropriate communications or threats at the federal level. In that event, information concerning the individuals provided by the state and local agencies assists the USMS in assessing the dangers they pose to federal officials and in developing protective measures and responding to specific security requirements. This information also assists in researching inappropriate communications directed toward judicial officials of all jurisdictions to gain a full and comprehensive picture of the diverse circumstances involved, to analyze trends based on a statistically reliable study, and to more fully address the problem.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records or information may be disclosed:

- (a) Where a record, either alone or in conjunction with other information, indicates a potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, territorial, local, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;
- (b) To other law enforcement agencies to develop protective measures where a specific threat is posed to their members; and to an individual or organization where the recipient is or may become the target of a specific threat;
- (c) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;
- (d) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;
- (e) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;
- (f) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;
- (g) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings;
- (h) To federal, state, territorial, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit;
- (i) A record may be disclosed to designated officers and employees of state, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with

hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer, detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision;

(j) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;

(k) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft, fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Paper records are kept in file folders. Duplicate copies of paper records are stored on microfilm discs.

Retrievability:

Records are retrieved by name and identifying number or a combination of the name and number.

Safeguards:

Except as otherwise noted in paragraphs (a) and (b) under "Routine uses," access to computerized records is restricted to personnel in the Investigative Services Division and each district office by user identification and password. Paper records are maintained in cabinets within supervised areas. District and headquarters offices are locked during work and non-duty hours and entry is restricted to employees with official identification.

Retention and disposal:

Headquarters files are destroyed one year after the initiator of the threat or inappropriate communication is no longer active or the case has been closed. District files are destroyed two years after the initiator of the threat or inappropriate communication is no longer active or the case has been closed.

System manager(s) and address:

Assistant Director, Investigative Services Division, U.S. Marshals Service, CS-4, Washington, DC 20530-1000.

Notification procedure:

Same as "Record access procedure."

Record access procedures:

Make all requests for access in writing and clearly mark letter and envelope "Freedom of Information/Privacy Act Request." Clearly indicate name of the requester, nature of the request sought, approximate date of the record, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above, Attention: FOIA Officer, and provide a return address for transmitting the information.

Contesting record procedures:

Direct all requests to contest or amend information to the system manager identified above. State clearly and concisely the information being contested, the reason for contesting it, and the proposed amendment to the information sought. Clearly mark the letter and envelope "Freedom of Information/Privacy Act Request."

Record Source Categories:

Information is obtained from public and confidential sources, the threat or inappropriate communication initiator, and from federal, state and local law enforcement agencies.

Exemptions claimed for the system:

The Attorney General has exempted this system from subsections (c)(3) and (4), (d), (e) and (3), (e)(4)(G) and (H), (e)(5), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S. 552a(j)(2). Rules have been promulgated in accordance with the requirements of 5 U.S. 553(b), (c) and (e) and have been published in the *Federal Register*. See 28 CFR 16.10

[\[TOP\]](#)

JUSTICE/USM-010

System name:

Judicial Facility Security Index System.

Security classification:

Limited Official Use.

System location:

Judicial Security Division, United States Marshals Service (USMS), CS-3, Washington, 20530-1000.

Categories of individuals covered by the system:

Individuals employed, or offered employment as contract court security officers (CSO's)

companies contracting with the USMS to provide judicial area security in federal courthouses and USMS facilities.

Categories of records in the system:

An alphabetical index contains the name, date of birth and social security number of the name of the contracting security firm (employer), completion dates and cost data for limited background investigation and orientation, district of employment, dates contract performance started and ended, posts and hours of duty and the status of employment, i.e., active or inactive. For inactive CSO's, the index contains the reason for inaction, e.g., CSO resigning, applicant rejected based on the preliminary records check; CSO removed based on Offense Personnel Management (OPM) background investigation; etc. In addition to providing abbreviated data, the index assists in locating records on the CSO related to the initial screening process for eligibility, e.g., application and preliminary checks for arrest records which are filed under the contract number and name of the contracting security firm (employer). The index also assists in locating files containing OPM reports on the limited background investigation and internal suitability memoranda which are segregated by categories "active" and "inactive."

Authority for maintenance of the system:

28 U.S.C. 509, 510 and 561 *et seq.*; 5 U.S.C. 301; 44 U.S.C. 3101 and 28 CFR 0.111.

Purpose(s):

The USMS administers and implements courtroom security requirements for the federal judiciary and provides assistance in the protection of federal property and buildings. The Judicial Facility Security Program provides uniformed security officers and security systems and equipment for judicial area security in federal courthouses throughout the country. It is funded by the Judiciary through the Administrative Office of the U.S. Courts (AOUSC) and is managed by the USMS. This system of records is used to make security/suitability determinations in the hiring of CSO's, to monitor orientation and training, to track costs for background investigations and attendance at Government-sponsored orientation, and to monitor contractor performance. It enables program officers to compile data for reports to the AOUSC on actual and projected expenses, to list CSO's, their posts and hours of duty, to determine turnover and reemployment ratios among CSO's.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records may be disclosed as follows:

(a) To any criminal, civil, or regulatory law enforcement authority (whether federal, state territorial, local, tribal, or foreign) where the information is relevant to the recipient entity enforcement responsibilities;

(b) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(c) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(d) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(e) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(f) To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings;

(g) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit;

(h) A record may be disclosed to designated officers and employees of state, territorial,

(including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prison detainees, to the extent that the information is relevant and necessary to the recipient agency decision;

(i) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;

(j) To a former employee of the Department for purposes of: responding to an official inquiry from a federal, state, territorial, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(k) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft, fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

An index record is stored on magnetic disks and original paper records are kept in file folders.

Retrievability:

Records are retrieved by name of the contract CSO or contractor.

Safeguards:

Records are stored in locked metal filing cabinets during off-duty hours. Access to computerized records is controlled by restricted code to personnel on a need-to-know basis. Entry to USMS Headquarters is restricted by 24-hour guard service to employees with official photo and electronic identification.

Retention and disposal:

Records are maintained indefinitely until a detailed records retention plan and disposal schedule is developed by the National Archives and Records Administration and the USMS.

System manager(s) and address:

Chief, Judicial Facility Security Program, Judicial Security Division, U.S. Marshals Service, CS-3, Washington, DC 20530-1000.

Notification procedures:

Same as the "Record access procedures."

Record access procedures:

Make all requests for access in writing and clearly mark the letter and envelope "Freedom of Information/Privacy Act Request." Clearly indicate name of the requester, nature of the request sought, approximate dates of the record, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above, Attention: Freedom of Information Officer, and provide a return address for transmitting the information.

Contesting record procedures:

Direct all requests to contest or amend information to the system manager listed above. Clearly and concisely the information being contested, the reasons for contesting it, and proposed amendment to the information sought. Clearly mark the letter and envelope "Freedom of Information/Privacy Act Request."

Record source categories:

Information contained in this system is collected from the individual, USMS orientation and other law enforcement agencies, OPM and from the contractor (employer).

Exemptions claimed for the system:

The Attorney General has exempted this system from subsections (c)(3) and (d) of the Information Privacy Act pursuant to 5 U.S.C. 552a(k)(5). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c) and (e) and have been published in the *Federal Register*. See 28 CFR 16.101.

[\[TOP\]](#)

JUSTICE/USM-011

System name:

Judicial Protection Information System.

Security classification:

Limited Official Use.

System location:

Primary System: Judicial Security Division, United States Marshals Service (USMS), CS-1, Washington, DC 20530-1000.

Decentralized Segments: Each USMS district office maintains their own files. The addresses of the USMS district offices are available on the Internet at <http://www.usdoj.gov/marshals/umsofc.aspx>.

Categories of individuals covered by the system:

Individuals who have been directly threatened or are subject to violent threat by virtue of responsibilities within the judicial system, e.g., U.S. Attorneys and their assistants, federal jurists and other court officials.

Categories of records in the system:

Manual and automated indices contain abbreviated data, e.g., case number, name of person subject, name of control district and district number, an indication of the type and source of threat, and the means by which the threat was made. In addition to the abbreviated data named above, the complete file may contain descriptive physical data of the protectee, and other information to identify security risks and plan protective measures in advance of or during periods of active protection, e.g., individual practices and routines, including association with other persons and memberships. Information regarding the expenditure of funds and allocation of resources assigned to the protectee may also be included in the file to enable officials to develop and implement operating plans to counteract threat situations.

Authority for maintenance of the system:

28 U.S.C. 509, 510 and 561 *et seq.*, 5 U.S.C. 301; 44 U.S.C. 3101; and 28 CFR 0.111 (c) through (f).

Purpose:

The USMS is required to protect U.S. Attorneys and their assistants, federal jurists and court officers; to provide for courtroom security, and to assist in protecting federal proper buildings. This operation requires obtaining information to allow an accurate assessment of individual security needs of such threatened persons to aid in developing protective measures and advance planning of specific security assignments. With the information collected, officials determine and carry out operating plans, funding, personnel assignments and use of special resources needed to counteract specific threat situations.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records or information may be disclosed:

- (a) To other federal, state and local law enforcement agencies to the extent that disclosure is necessary to develop and/or implement protective measures;
- (b) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;
- (c) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;
- (d) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;
- (e) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;
- (f) To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings;
- (g) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;
- (h) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, territorial or local government entity or professional licensing authority in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes when the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;
- (i) To any criminal, civil, or regulatory law enforcement authority (whether federal, state,

territorial, local, tribal, or foreign) where the information is relevant to the recipient entity enforcement responsibilities;

(j) To appropriate agencies, entities, and persons when (1) the Department suspects or confirmed that the security or confidentiality of information in the system of records has compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (w maintained by the Department or another agency or entity) that rely upon the compromi information; and (3) the disclosure made to such agencies, entities, and persons is reas necessary to assist in connection with the Department's efforts to respond to the susper confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

An index record is stored on index cards and magnetic tape. Original paper records are file folders.

Retrievability:

Records are indexed and retrieved by name of protectee.

Safeguards:

Access to computerized records is restricted to Court Security Program personnel by as user code and password. In addition, records are stored in locked metal cabinets during off-duty hours. The records are located in a restricted area, and USMS Headquarters is 24-hour guard protection with entry controlled by official and electronic identification.

Retention and disposal:

Records are maintained indefinitely until a detailed records retention plan and disposal schedule is developed by the National Archives and Records Administration and the US

System manager(s) and address:

Chief, Court Security Program, Judicial Security Division, U.S. Marshals Service, CS-3, Washington, DC 20530-1000.

Notification procedure:

Same as the "Record access procedures."

Record access procedures:

Make all requests for access in writing and clearly mark letter and envelope "Freedom of Information/Privacy Act Request." Clearly indicate the name of the requester, nature of record sought, approximate dates of the record, and provide the required verification of (28 CFR 16.41(d)). Direct all requests to the system manager identified above, Attention FOI/PA Officer, and provide a return address for transmitting the information.

Contesting record procedures:

Direct all requests to contest or amend information to the system manager identified above. State clearly and concisely the information being contested, the reason for contesting it, and the proposed amendment to the information sought. Clearly mark the letter and envelope "Freedom of Information/Privacy Act Request."

Record source categories:

Information is obtained from individual protectees; federal, state, and local law enforcement agencies; public and confidential sources; and threat initiator.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

JUSTICE/USM-013

System name:

U.S. Marshals Service Administrative Proceedings, Claims and Civil Litigation Files

Security Classification:

Limited Official Use

System location:

Office of General Counsel, U.S. Marshals Service (USMS), CS-3, Washington, DC 20530-1000.

Categories of individuals covered by the system:

Individuals who have filed tort and employee claims against the USMS; individuals who initiated administrative proceedings against the USMS; individuals who have filed civil suits naming the USMS and/or personnel as defendants, including those suits arising from authorized criminal law enforcement activities; individuals named as defendants in federal actions initiated by the USMS; and USMS attorneys assigned to defend such claims and litigation.

Categories of records in the system:

In addition to the names of individuals covered by the system and the title of cases, a computerized case tracking system contains certain summary data, e.g.; a summary of correspondence and pleadings received in a case, names of parties involved; names of attorneys handling the case or matter, court in which action is brought, and civil action number thereby facilitating location of the complete file. Cases or matters include adverse action grievances, unfair labor practice charges, tort claims, Equal Employment Opportunity and other employee claims, and suits against USMS employees in their official capacities, and contain correspondence/claim forms submitted by claimants and internal reports and records documents concerning the merits of the claim, attorney or staff recommendations and file

related to the claim; records on actions taken by USMS giving rise to appeals, attorney recommendations and strategy for defending appeals; copies of civil actions filed and criminal investigative records related to the action, e.g., criminal investigative reports relating to the underlying criminal matter which relates to or constitutes the basis of the claim or suit (including those from non-Federal law enforcement participants in USMS criminal or civil enforcement activities), witness statements, reports of interviews, exhibits, attorney notes, pleadings, and recommendations and strategy for defending civil actions.

Authority for maintenance of the system:

5 U.S.C. 301 and 44 U.S.C. 3101.

Purpose(s):

Among other responsibilities, the Office of General Counsel, U.S. Marshals Service, provides legal representation to USMS management in all administrative matters including, but not limited to, adverse actions, grievances, unfair labor practices, EEO, tort and employee compensation proceedings; represents the Service and its employees in district court actions brought against them for acts taken in the course of official duties; and represents the Service in other actions in which its interests are involved. Effective representation in such matters requires that records be retrievable by individual identifiers.

Routine uses of records maintained in the system including categories of users and purposes of such uses:

Records maintained in this system of records may be disseminated as follows:

- (a) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, territorial, local, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;
- (b) To any federal, state or local agency, organization or individual to the extent necessary to elicit information or witness cooperation if there is reason to believe the recipient possesses information related to the case or matter;

(c) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(d) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit;

(e) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings;

(f) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(g) To the news media and the public including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(h) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(i) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(j) A record may be disclosed to designated officers and employees of state, territorial, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners;

detainees, to the extent that the information is relevant and necessary to the recipients agency's decision;

(k) To a former employee of the Department for purposes of: responding to an official in by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(l) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Administrative claim, appeal, and litigation files are stored in standard file cabinets. The computerized case tracking system and duplicate copies of some paper records are stored on magnetic discs.

Retrievability:

Records are retrieved by name of claimant, litigant or USMS attorney, or by caption of case or action or administrative proceeding.

Safeguards:

Access to computerized records is restricted to Office of General Counsel personnel by

identification and passwords. In addition, files are stored in metal filing cabinets within the Office of General Counsel, USMS Headquarters during off-duty hours. Access to USMS Headquarters is restricted to employees with official identification.

Retention and disposal:

Records in the case tracking system are retained indefinitely. Claim files are destroyed 5 years. Litigation files are destroyed after 10 years. Cases designated by the General Counsel as significant or precedential are retained indefinitely.

System manager(s) and address:

General Counsel, Office of General Counsel, U.S. Marshals Service, CS-3, Washington, DC 20530-1000.

Notification procedure:

Same as "Record access procedures."

Record access procedures:

Make all requests for access in writing and clearly mark letter and envelope "Freedom of Information/Privacy Act Request." Clearly indicate name of the requester, nature of the information sought, approximate dates of the records, and provide the required verification of identity (28 CFR 16.41(d)). Direct all requests to the system manager identified above. Attention: FOIA Officer, and provide a return address for transmitting the information.

Contesting record procedures:

Direct all requests to contest or amend information to the system manager listed above. Clearly and concisely what information is being contested, the reason for contesting it, and a proposed amendment to the information sought. Clearly mark the letter and envelope "Freedom of Information/Privacy Act Request."

Record source categories:

The sources of information contained in this system are the individual claimant/litigant, the

officials, law enforcement agencies, statements of witnesses and parties, transcripts of depositions and court proceedings, administrative hearings and arbitrations, and work product of staff attorneys and legal assistants working on a particular case or matter.

Exemptions claimed for the system:

The Attorney General has exempted certain categories of records in this system from subsections (c)(3) and (4); (d); (e)(2) and (3); (e)(4)(G) and (H); (e)(8); (f) and (g) of the Act pursuant to 5 U.S.C. 552a(j)(2) or (k)(5). The system is exempted pursuant to subsection (j)(2) only to the extent that information in a record pertaining to a particular individual relates to a criminal investigation which relates to or constitutes the basis of a particular suit or claim. The system is exempted pursuant to subsection (k)(5) only to the extent necessary to protect a confidential source. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and have been published in the *Federal Register*. See 28 CFR 16.101.

[\[TOP\]](#)

JUSTICE/USM-014

System name:

Joint Automated Booking Stations (JABS), USM-014.

System location:

U.S. Marshals Service (USMS) headquarters, 600 Army Navy Drive, Arlington, Va. 22204; and regional office of the Drug Enforcement Administration (DEA) at 6320 NW 2nd Avenue, North Miami Beach, FL 33167.^{1 1}

The Miami repository will be physically housed at DEA facilities; nevertheless, management and oversight—including the physical security of the system—will be the responsibility of USMS personnel. When appropriate, the "system location" will be revised to include additional repositories.

Categories of individuals covered by the system:

Alleged criminal offenders who have been arrested and booked.

Categories of records in the system:

Records may include certain generic or "common" data elements which have been collected by an arresting Federal, State, or local agency and booked by that agency at its automated booking station (ABS), or booked by an agency on behalf of another agency which performed the arrest.² Such common data (approximately 60 data elements) have been identified by law enforcement as those case and biographical data generally collected by the law enforcement community during booking arrests, e.g., name, date and place of birth, citizenship, hair color, eye color, height and weight, occupation, social security number, place, date and time of arrest, and jail location, charge, armed description, sentenced or unsentenced, and health status. Such data may also include case agent name, notes and observations regarding subject's physical or mental condition, degree of psychological stability or acumen, reported use of or forming substances, substances for which the subject has a valid prescription, names of contacts or individuals from which the subject is to be segregated, extraordinary handling procedures, and include precautionary warnings, names of acquaintances (criminal/non-criminal), Federal and State identification numbers, and any other pertinent information related to known activities relevant or unique to the subject. Finally, as the technology is developed, such data may include electronic fingerprint mugshots, and voice samples.²

Initially, these records will include only those of the Department of Justice (DOJ) law enforcement components. However, at such time as other Federal, State and local agencies either establish similar ABS's or use the ABS of another agency to upload "common" data into the repositories (i.e., "common" data as described by this system of records), this system of records will also include records provided by non-DOJ law enforcement agencies.

Categories of records may include paper records where the USMS has a need to print copies, e.g., copies of mugshots.

Authority for maintenance of the system:

28 U.S.C. 534, 564; 5 U.S.C. 301 and 44 U.S.C. 3101.

Purpose(s):

The primary purpose of the JABS system is to enable Federal, State, and local agencies conduct arrests and/or booking activities to store such data in regional repositories to eliminate duplication efforts among multiple law enforcement agencies participating in a single booking/arrest, to follow the arrestee through the booking process, and thereby share "realtime" booking and arrest data within a region. It will also assist in ancillary law enforcement efforts by permitting law enforcement to learn of the arrest and apprehend a fugitive by another agency in that region; verify the identity of an arrestee or, as the technology is developed, obtain identifying data that will assist with surveillance and wiretap activities in the event the arrestee becomes a fugitive subsequent to booking. Finally, it may assist judicial/law enforcement agencies in obtaining such information as will permit them to perform their official duties.

JABS will also assist law enforcement at the national level through interface of its regional repositories with the Federal Bureau of Investigation's (FBI) Identification Division Record System, Justice/FBI-009 (IDENT). IDENT currently serves as a "national" repository for fingerprint data. As the technology is developed, electronic fingerprint, mugshot, and voice sample data, together with certain personally identifying data, date of arrest, etc. may be copied from JABS regional repositories to IDENT. (Consistent with published routine use disclosures for the IDENT system of records, IDENT may then respond to electronic inquiries from other JABS regional repositories to verify fingerprint or other identifying data, to locate the arrest of a fugitive in another regional jurisdiction; and/or, where indicated by the IDENT record, to allow an inquiring regional repository to determine that a more complete arrest record resides with, and may be requested from, another JABS regional repository; and otherwise assist in the conduct of other authorized law enforcement activities such as surveillance and wiretap.)

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

(a) The regional repositories may be electronically accessed by Federal, State, and local law enforcement agencies to input and retrieve booking and arrests data on criminal offenders, thereby eliminate the need for duplicate bookings in that region, i.e., the collection of the same data by multiple agencies in prisoner processing activities involving such agencies' arrest through incarceration. (For example, an individual arrested by the Bureau of Alcohol, Tobacco, and Firearms (ATF) and transported by the USMS to a Federal correctional institution may be processed by ATF, USMS, and the Bureau of Prisons.) Such repositories may be

electronically accessed by these and other local law enforcement agencies in the region for other law enforcement purposes such as to learn about the arrest of a fugitive wanted in several local jurisdictions, to verify the identity of an arrestee, or to assist in the conduct of surveillance and/or wiretap activities. In addition, access by one regional repository to the complete record residing in another regional repository, e.g., to obtain access to the record of a fugitive wanted in one or more regional jurisdictions, may be accomplished by a telephone request until such time as technology may permit electronic requests between regional repositories. Further, at such time as the technology is available, other judicial/law enforcement agencies such as the courts, probation, and parole agencies may have direct electronic access to JABS in order to obtain data which may assist them in performing their official duties. For example, the courts may need direct electronic access to verify the identity of an individual who appears in court claiming not to be the individual identified by the arresting agency.

Finally, where necessary and/or appropriate, the USMS may disclose relevant information to the repositories as follows:

- (b) To any Federal, State, and/or local authorities to the extent necessary to permit them to perform their law enforcement responsibilities; or to any Federal, State, and/or local authority or to any other entity or person, to the extent required to solicit information necessary for law enforcement purposes;
- (c) To other judicial/law enforcement agencies such as the courts, probation, and parole agencies to assist them in performing their official duties;
- (d) To a Federal agency in response to its request and in connection with hiring or reemployment of an employee, the issuance of the required security clearance, the reporting of an investment of an employee, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter;
- (e) To private contractors and/or maintenance personnel but only to the extent that access is needed to perform contractual duties such as maintenance or other administrative support operations;
- (f) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of and at the request of the individual who is the subject of the record;

(g) To the news media and the public pursuant to 28 CFR 50.2 unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(h) To a court or adjudicative body before which the USMS or other appropriate DOJ component is authorized to appear when any of the following is a party to litigation or has an interest in litigation and such records are determined by the USMS or other appropriate component to be arguably relevant to the litigation: (i) The USMS or DOJ component, or subdivision thereof, or (ii) any employee of the USMS or DOJ in his or her official capacity, or (iii) any employee of the USMS or DOJ in his or her individual capacity where the DOJ has agreed to represent the employee, or (iv) the United States, where the DOJ determines that litigation is likely to affect it or any of its subdivisions;

(i) To the National Archives and Records Administration (NARA) and the General Services Administration in records management inspections conducted under the authority of 44 CFR 2904 and 2906;

(j) To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of an investigation (e.g. an arrest) arising from the matters of which they complained and/or of which they were a victim; and

(k) To any person or entity to the extent necessary to prevent an imminent and potential harm which directly threatens loss of life or serious bodily injury.

Pursuant to subsection (b)(3) of the Privacy Act, the Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are stored in computerized media and on printed copy.

Retrievability:

Data may be retrieved by name or identifying number.

Safeguards:

Access will be limited to those with a need to know. Facilities and offices which house computer systems will be protected at all times by appropriate locks, security guards, and alarm systems. Access to the systems equipment is limited to those with a need-to-know through encryption and password protection measures.

Retention and disposal:

A disposition schedule will be developed for approval by the USMS Records Management Officer and NARA. Upon approval of such schedule, this notice will be revised to reflect correct retention and disposal schedule for these records.

System manager(s) and address:

Director, U.S. Marshals Service, 600 Army-Navy Drive, Arlington, Virginia 22202-4210

Notification procedure:

Same as "Record Access Procedures."

Record access procedure:

Address all requests for access to JABS records, in writing, to the system manager identified above, "Attention: FOI/PA Officer." Clearly mark the letter and envelope "Privacy Act request." Clearly indicate the name of the requester, nature of the record sought, and approximate date of the record. In addition, provide the required verification of identity (28 CFR 16.41(d)) and return address for transmitting the information.

Contesting records procedure:

Same as above.

Record source categories:

The record subject; Federal, State, and local law enforcement personnel; the courts; and medical personnel.

Systems exempted from certain provisions of the act:

The Attorney General has exempted records in this system from subsections (c) (3) and (d), (e) (1), (2) and (3), (e)(5), (e)(8), and (g) of the Privacy Act pursuant to 5 U.S.C. 552. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553 (b), (e) and have been published in the *Federal Register*.

[\[TOP\]](#)

JUSTICE/USM-015

SYSTEM NAME:

U.S. Marshals Service (USMS) Employee Assistance Program (EAP) Records.

SECURITY CLASSIFICATION:

Limited official use.

SYSTEM LOCATION:

Primary system: Human Resources Division, U.S. Marshals Service, CS-3, Washington 20530-1000. Contractor records are maintained at the respective offices of these providers. These addresses may be obtained by contacting the USMS Employee Assistance Program (EAP) Office.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former employees of the USMS (and in limited cases, immediate family members who have sought counseling or have been referred for counseling or treatment through USMS EAP. The remainder of this notice will refer to all persons covered by this system "EAP client(s)" .

CATEGORIES OF RECORDS IN THE SYSTEM:

Records include any record, written or electronic, which may assist in diagnosing, evaluating counseling and/or treating an EAP client; or resolving an EAP client's complaint and/or management's concern (management consultation) regarding the EAP client's performance, attendance, or conduct issues. The records may contain the consent forms; intake/term and outcome documents; case notes; pertinent psychosocial, medical and employment histories; medical tests or screenings, including drug and alcohol tests and information on positive drug tests generated by the Drug Free Workplace Program or treatment facilities; treatment and rehabilitation plans and recommendations; abeyance/back-to-work agreements; insurance data; behavioral improvement plans; and referral records. Where clinical referrals have been made, records may include information related to counseling, diagnosis, prognosis, treatment and evaluation, together with follow-up data that may be generated by the provider providing the services. Records may also include those that can assist in the monitoring, managing, and evaluating the contractor's performance such as sanitized audit records of the EAP/Contractor Program.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 290dd, *et seq.* and 290ee, *et seq.*; 42 CFR 2.1, *et seq.*; E.O. 12564, 5 U.S.C. 552 and 7901; 44 U.S.C. 3101 and Public Law 100-71, sec. 503 (July 11, 1987).

PURPOSE(S):

The EAP is a voluntary program designed to assist clients in obtaining help in handling personal problem(s) affecting job performance, and to provide emotional support and assistance during periods of crises. Records are maintained to document and monitor client participation in the EAP program; to monitor compliance with abeyance and back-to-work agreements; to document the nature and effects of the employee's personal problem(s); to manage and monitor contractor performance. Routine uses of records maintained in the system, including categories of users and the purpose of such uses:

Records or Information May be Disclosed:

- (a) To appropriate state or local authorities to report, where required under state law, information of suspected child, elder or domestic abuse or neglect;
- (b) To any person or entity to the extent necessary to prevent an imminent crime which threatens loss of life or serious bodily injury;
- (c) To USMS contractors that provide counseling and other services through referrals from EAP staff to the extent that it is appropriate, relevant, and necessary to enable the contractors to perform counseling, treatment, rehabilitation, and evaluation duties;
- (d) To any person responsible for the care of an EAP client when the EAP client to whom the records pertain is mentally incompetent or under legal disability;
- (e) To any person or entity to the extent necessary to meet a bona fide medical emergency;
- (f) To appropriate agencies, entities, and persons when (1) The Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to Consumer Reporting Agencies:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Information is stored in locked metal safes and in computerized databases.

RETRIEVABILITY:

Records are retrieved by name of employee and, in limited cases immediate family members.

SAFEGUARDS:

In accordance with the requirements of 42 CFR 2.16, USMS EAP, contractor records are maintained in a secure environment. Access to USMS EAP records is restricted to designated USMS personnel, except as otherwise permitted by law or with the written consent of the individual. Payment Vouchers prepared to effect payment for services rendered by the contractors in performance of the contract do not contain individual identifiers. Invoices prepared by contractors located outside the Washington, DC metropolitan area are sent by first-class mail to the designated member(s) of the local contractors contracted with the USMS. In turn, invoices or other documents prepared in support of payment vouchers which contain individual identifiers are hand-carried by the local contractors to the EAP Administrator who retains the supporting documents. Records are maintained in locked metal safes. Entry to headquarters is restricted by 24-hour guard service to employees with official and electronic identification.

Access to contractors records is restricted to a designated member(s) of the contractors as otherwise provided by law or with the written consent of the individual. Contractors records are stored in locked files also.

RETENTION AND DISPOSAL:

Records, paper or electronic, are retained for three years after the individual ceases contact with the USMS EAP and/or the contractor unless a longer retention period is necessary because of pending administrative or judicial proceedings. In such cases, the records are retained for six months after the case is closed. At that time the records are destroyed by shredding (General Records Schedules 26 and 36).

SYSTEM MANAGER(S) AND ADDRESS:

Employee Assistance Program Administrator, Health and Safety Team, Human Resources Division, United States Marshals Service, CS-3, Washington, DC 20530-1000.

NOTIFICATION PROCEDURE:

Same as "Record access procedures."

RECORD ACCESS PROCEDURES:

Address all requests for access to the USMS EAP records in writing to system manger identified above. Address all requests for records maintained by the contractor to these providers. Address(es) of these service providers may be obtained by contacting the US EAP Office. Clearly mark the envelope and letter "Privacy Act Request." Clearly indicate name of the requester, nature of the record sought, and approximate date of the record addition, provide the required verification of identity (28 CFR 16.41(d)) and a return add transmitting the information.

CONTESTING RECORD PROCEDURES:

Direct all requests to contest or amend information in accordance with the procedures c under "Record access procedures." State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment to the informatio sought. Clearly mark the letter and envelope "Privacy Act Amendment Request."

RECORD SOURCE CATEGORIES:

Records are generated by the EAP client who is the subject of the record; USMS EAP personnel; the contractors, and the specialized service providers; the USMS Human Re Division; and the employee's supervisor. In the case of a confirmed, unjustified positive test, records may also be generated by the staff of the Drug-Free Workplace Program a Medical Review Officer.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[\[TOP\]](#)

JUSTICE/USM-016

System name:

U.S. Marshal Service (USMS) Key Control Record System.

Security classification:

Limited Official Use.

System location:

Primary system: Judicial Security Division, United States Marshals Service, CS-3, Wash DC 20530.

Decentralized segments: USMS headquarters division offices that issue keys to their respective employees.

Categories of individuals covered by the system:

Current and former employees of the USMS who have been issued building or office keys at USMS Headquarters or District Office locations.

Categories of records in the system:

Records contained in this system consist of an automated or manual index which may include the name of the employee to whom a building or office key is issued; the social security number (only when two or more employees have identical names, including middle initials); unique key identification code number; key type (e.g., grand master, master, submaster, change); storage container hook number; description (e.g., number identification) of door, room(s), and/or area(s) the key opens or accesses; transactions type and/or status (e.g., issued, transferred, retrieved, lost, broken) and transaction date; and, any other appropriate comment, e.g., comments regarding key, door, room, area, etc.

Authority for maintenance of the system:

5 U.S.C. 301 and 44 U.S.C. 3101.

Purpose(s):

The USMS Key Control Record System serves as a record of keys issued and facilitates continuing security at USMS Headquarters locations. Records are maintained to assist in restricting office and work area access to authorized USMS personnel by controlling, monitoring and tracking keys issued. In addition, the records assist in identifying any rechanges, or additional security measures that may be necessary as a result of lost or broken keys.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

Records or information may be disclosed:

(a) Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or enforcing or charged with implementing such law;

(b) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(c) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records.

(d) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(e) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(f) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(g) To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings;

(h) To a former employee of the Department for purposes of: responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with former employee that may be necessary for personnel-related or other official purposes the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(i) To appropriate agencies, entities, and persons when (1) the Department suspects or confirmed that the security or confidentiality of information in the system of records has compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of in the system:

Storage:

Automated index records are stored on magnetic disks. Paper copies of automated records are kept in file folders and original paper records of the manual index are stored in card files.

Retrievability:

Records are retrieved by name of the individuals covered by the system.

Safeguards:

Access to these records is restricted to personnel of the USMS, Office of Security. Computerized records may be accessed only by assigned code and password. Paper records are located in a restricted area and are maintained in metal filing cabinets or safes which are locked during non-duty hours.

Retention and disposal:

Records are retained for three years after turn-in of the key at which time they are destroyed (General Records Schedule 18).

System manager(s) and address:

Judicial Security Division, United States Marshals Service, CS-3, Washington, DC 20535

Notification procedure:

Same as the "Records access procedures."

Record access procedures:

Make all requests for access in writing and clearly mark letter and envelope "Freedom of Information/Privacy Act Request." Clearly indicate the name of the requester, nature of the record sought, approximate dates of the record, and provide the required verification of (28 CFR 16.41(d)). Direct all requests to the system manager identified above, Attention: FOI/PA Officer, and provide a return address for transmitting the information.

Contesting record procedures:

Direct all requests to contest or amend information to the system manager listed above. Clearly and concisely state the information being contested, the reasons for contesting it, and the proposed amendment to the information sought. Clearly mark the letter and envelope

"Freedom of Information/Privacy Act Request."

Record source categories:

Information contained in this system is collected from the individual and the system mar

Exemptions claimed for the system:

None.

[\[TOP\]](#)

JUSTICE/USM-017

System Name:

Judicial Security Staff Inventory.

Security classification:

Limited Official Use.

System location:

Judicial Security Division (JSD), U.S. Marshals Service (USMS), CS-3, Washington, DC 20530-1000.

Categories of individuals covered by the system:

USMS employees, contract employees, and other individuals assigned to JSD.

Categories of records in the system:

Records contained in this computerized system consist of (1) an individual's name, date birth, social security number, and type of passport with expiration date; (2) inventory of accountable property assigned to individual, including: weapon, protective body armor, expiration date of warranty, vehicle, credit cards, cell phone, pager, and office equipment.

Authority for maintenance of the system:

5 U.S.C. 301; 28 U.S.C. 509 and 510; 44 U.S.C. 3101 and 28 CFR 0.111.

Purpose(s):

This system will be used to assist JSD management in the effective control of accountal property and to ensure that JSD personnel maintain the equipment necessary and in pr working order to perform their functions, especially law enforcement functions, and to r quickly to urgent operational law enforcement activities as they develop.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:***Records or information may be disclosed:***

- (a) Where a record, either alone or in conjunction with other information, indicates a viol potential violation of law—criminal, civil, or regulatory in nature—the relevant records m referred to the appropriate federal, state, territorial, local, tribal or foreign law enforceme authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;
- (b) In an appropriate proceeding before a court, grand jury, or administrative or adjudica body, when the Department of Justice determines that the records are arguably relevan proceeding; or in an appropriate proceeding before an administrative or adjudicative bo when the adjudicator determines the records to be relevant to the proceeding;
- (c) To the news media and the public, including disclosure pursuant to 28 CFR 50.2, ur is determined that release of the specific information in the context of a particular case v constitute an unwarranted invasion of personal privacy;
- (d) To a Member of Congress or staff acting upon the Member's behalf when the Memb staff requests the information on behalf of, and at the request of, the individual who is tl subject of the record;
- (e) To the National Archives and Records Administration for purposes of records manag

inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(f) To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings;

(g) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or its records;

(h) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(i) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft, fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are kept in a computerized database.

Retrievability:

Information is retrieved by name and social security number.

Safeguards:

Access is limited to designated staff of JSD by assigned user code and password. JSD located in a restricted area of USMS Headquarters which is under 24-hour guard protection with entry controlled by official and electronic identification.

Retention and disposal:

Files are maintained until the employee leaves JSD at which time all records on the individual will be erased from the database.

System manager(s) and address:

Assistant Director, Judicial Security Division, U.S. Marshals Service, CS-3, Washington, DC 20530-1000.

Notification procedure:

Same as the "Record access procedures."

Record access procedures:

Make all requests for access in writing and clearly mark letter and envelope "Privacy Access Request." Clearly indicate the name of the requester, nature of the record sought, approximate dates of the record, and provide the required verification of identity (28 CFR 16.41(d)). Forward requests to the system manager identified above, attention: FOI/PA Officer, and provide return address for transmitting the information.

Contesting record procedures:

Direct all requests to contest or amend information to the system manager identified above.

State clearly and concisely the information being contested, the reasons for contesting the proposed amendment to the information sought. Clearly mark the letter and envelope "Privacy Act Request."

Record source categories:

Information is obtained from subject JSD employees, JSD office and the accountable personnel records.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

JUSTICE/USM-018

System name:

United States Marshals Service Alternative Dispute Resolution (ADR) Files and Database Tracking System.

Security classification:

Limited official use.

System location:

Human Resources Division, United States Marshals Service (USMS), CS-3, Washington 20530-1000.

Categories of individuals covered by the system:

Employees of the USMS designated as complainants, who select ADR mediation as the mechanism to resolve disagreements, and designated respondents to such complaints.

Categories of records in the system:

ADR files contain a statement of issue(s) which include type of dispute, parties involved date ADR requested or notified by complainant; mediator appointed; correspondence or which may include ground rules, acknowledgment of time requirements and issues related thereto; pre-conference agreements; minutes of ADR activity; written agreement, and date of resolution and date resolved.

The ADR data tracking system contains names of complainant and respondent; type of dispute, e.g., job assignment, leave, promotion; source of complaint, e.g., Equal Employment Opportunity (EEO) or grievance; process utilized, e.g., mediation, conciliation, fact finding; district/office; ADR contact individual; date ADR request received; date resolved; and calculation of time spent in resolving matters and, if applicable, name of mediator.

Authority for maintenance of the system:

5 U.S.C. 301 and 44 U.S.C. 3101.

Purpose(s):

The ADR process is a parallel system to the grievance process and Equal Employment Opportunity (EEO) complaint process which offers the possibility of a simpler, quicker, less expensive, and less adversarial resolution of disputes. The ADR files are used to facilitate effective operation of the ADR process in resolving discrimination complaints and workplace grievances by USMS employees and applicants for employment. The ADR database is used to track case activity, primarily for completion of reports.

Routine uses of records maintained in the system, including categories of users and purposes of such uses:

Records or information may be disclosed:

(a) Where a record, either alone or in conjunction with other information, indicates a potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, territorial, tribal or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;

(b) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body;

body, when the Department of Justice determines that the records are arguably relevant proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding;

(c) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(d) To a Member of Congress or staff acting upon the Member's behalf when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(e) To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906;

(f) To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings;

(g) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit;

(h) A record may be disclosed to designated officers and employees of state, territorial, (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prison detainees, to the extent that the information is relevant and necessary to the recipient agency's decision;

(i) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or

records;

(j) To a former employee of the Department for purposes of: responding to an official in a Federal, state, or local government entity or professional licensing authority, in accord with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(k) To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft, fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

Records in this system are not appropriate for disclosure to consumer reporting agencies.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Records are stored in standard file cabinets. Computerized records are stored in a data server in a secured file room.

Retrievability:

Records are retrieved by name of employee.

Safeguards:

Access is restricted to authorized personnel with the need to know in the Human Resources Division, Equal Employment Opportunity Division, and the Office of General Counsel. Computerized records may be accessed only by assigned code and password. In addition, records are stored in metal file cabinets within the Human Resources Division and access to USMS headquarters is controlled by 24-hour guard services.

Retention and disposal:

Records are maintained for 7 years and then data in the system, as well as hard copies, are purged.

System manager(s) and address:

Assistant Director, Human Resources Division, USMS, CS-3, Washington, DC 20530-1

Notification procedure:

Same as "Record access procedures."

Record access procedures:

Make all requests for access in writing and clearly mark letter and envelope "Privacy Act Request." Clearly indicate name of the requester, nature of the record sought, approximate dates of the records, and provide the required verification of identity (28 CFR 16.41(d)). Forward all requests to the system manager identified above, Attention: FOI/PA Officer, and provide return address for transmitting the information.

Contesting record procedures:

Direct all requests to contest or amend information to the system manager in accordance with the procedures outlined above. State clearly and concisely the information being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Employee complainants, who select the ADR process to resolve their disputes; respond to the ADR mediator.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

JUSTICE/USM-019

System name:

Merit Promotion Open Season Records System (MPOS), Justice/USM-019.

Security classification:

Limited Official Use.

System location:

United States Marshals Service (USMS) Headquarters, Washington, DC 20530-1000.

Categories of individuals covered by the system:

Individuals covered by the system include all permanent USMS criminal investigative employees, (GS-1811), interested in applying for promotions for positions at the GS-13 and above.

Categories of records in the system:

Records contain identifying data such as employee names, social security numbers, home work addresses, along with home and work phone numbers. Records also consist of an information necessary to rate qualifications and make selections including employees' work experience; service computation dates; performance appraisals; and current job titles, salaries and grades. All information is voluntarily submitted by the employees and their supervisors.

Authority for maintenance of the system:

5 CFR 335.103 and Department of Justice Order 1335b.

Purpose(s):

The MPOS supports the USMS merit promotion plan program by identifying and tracking interested and eligible employees in the event a vacancy announcement opens during the designated merit promotion period. The purpose of the merit promotion open season review system is to allow USMS 1811 criminal investigators to apply for positions during the year without waiting for vacancies to occur or new positions to be established and to, thereafter, receive consideration as positions become available. This system also assists the selecting officials in making valid selections.

Routine uses of records maintained in the system, including categories of users and purposes of such uses.

Records in this system may be disclosed:

- A. To the Office of Personnel Management (OPM) to enable that agency to conduct such review of USMS selections and the operation of the MPOS program as are consistent with OPM's statutory and regulatory authority.
- B. In an appropriate proceeding before a court, or administrative or adjudicative body, when the Department of Justice (DOJ) determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
- C. To an actual or potential party to litigation or the party's authorized representative for purpose of negotiation or discussion of such matters as settlement, plea bargaining, or informal discovery proceedings.
- D. To the Merit Systems Protection Board or the Office of the Special Counsel in connection with appeals, special studies of the civil service and other merit systems, review of office and regulations, investigations of alleged or possible prohibited personnel practices, and other functions, e.g., as prescribed in 5 U.S.C. Chapter 12, or as may be authorized by
- E. To the Equal Employment Opportunity Commission, when requested, in connection with investigations into alleged or possible discrimination practices in the Federal sector, examination of Federal affirmative employment programs, compliance by Federal agencies

the Uniform Guidelines or Employee Selection Procedures, or other functions vested in Commission.

F. To a Member of Congress, or staff acting upon the Member's behalf, when the Member's staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

H. To the Federal Labor Relations Authority or its General Counsel when requested in connection with investigations of allegations of unfair labor practices or matters before the Federal Service Impasses Panel.

I. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system or records.

J. To disclose information to an arbitrator to resolve disputes under a negotiated grievance procedure or to officials of labor organizations recognized under 5 U.S.C. Chapter 71 who are relevant and necessary to their duties of exclusive representation.

K. To the Union when required by contract as part of the processing of a grievance and an arbitrator in the arbitration of a grievance.

L. The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee if it may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

M. To appropriate officials and employees of a Federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an

employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit.

N. To any criminal, civil, or regulatory law enforcement authority (whether federal, state, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

O. To disclose information to any source from which additional information is requested to the extent necessary to identify the individual, inform the source of the purposes of the request, and to identify the type of information requested), when necessary to obtain information relevant to an agency decision concerning promoting or retaining an employee, issuing a security clearance, or conducting a security or suitability investigation of an individual.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of information in the system:

Storage:

Information is in paper and/or electronic format. The information is stored on computer tape, magnetic disks, and in file cabinets.

Retrievability:

Records may be retrieved by name, Social Security Number (SSN), or unique MPOS number.

Safeguards:

The USMS headquarters offices are located in buildings under security guard, and access to the premises is by official identification. Offices are locked during non-duty hours. Access to the system is obtained through remote terminals that require the use of restricted password and user ID. Paper records will be maintained in locked file cabinets. The MPOS server will be maintained in a secure computer facility.

Retention and disposal:

Records are retained for one year following the merit promotion open season announce for which they are submitted. Records are destroyed by shredding or burning.

System manager(s) and address:

Assistant Director, Human Resources Division, United States Marshals Service Headqu Washington, DC 20530-1000.

Notification procedure:

Inquiries should be addressed to the system manager.

Record access procedure:

A request for access to a record from this system shall be made in writing with the envelope and the letter clearly marked "Privacy Act Request." It should clearly indicate the name of the requester, the nature of the record sought and the approximate dates covered by the request. The requester shall also provide the required verification of identity as outlined in 28 CFR 16.41(d) and provide a return address for transmitting the information. Access requests directed to the System Manager listed above, Attention: FOI/PA Officer.

Contesting records procedure:

Individuals desiring to contest or amend information maintained in the system should direct their request to the System Manager listed above, stating clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought.

Record source categories:

Information contained in this system of records is obtained from the individuals covered by the system, or derived from information the individuals or their supervisors supplied.

Exemptions claimed for the system:

None.

[\[TOP\]](#)

JUSTICE/USM-999

Appendix to U.S. Marshals Service Systems of Records, Official Addresses of United States Marshals.

Northern Alabama

1729 5th Avenue, North, Room 240, Birmingham, Alabama 35203

Middle Alabama

PO Drawer 4249, Montgomery, Alabama 36103

Southern Alabama

PO Box 343, Mobile, Alabama 36601

District of Alaska

U.S. Courthouse & Federal Building, 222 W. 7th Avenue, No. 28, Anchorage, Alaska 99513-7568

District of Arizona

8204 U.S. Courthouse, 230 North First Avenue, Phoenix, Arizona 85025

Eastern Arkansas

PO Box 8, Little Rock, Arkansas 72203

Western Arkansas

PO Box 2625, Fort Smith, Arkansas 72902

Northern California

20005 U.S. Courthouse, 450 Golden Gate Avenue, San Francisco, California 94102

Eastern California

1020 U.S. Courthouse, 750 Capitol Mall, Sacramento, California 95814

Central California

U.S. Courthouse, 312 North Spring Street G-23, Los Angeles, California 90012-4798

Southern California

LLB-71 U.S. Courthouse, 940 Front Street, San Diego, California 92189

District of Colorado

Drawer 3599, Denver, Colorado 80294

District of Connecticut

PO Box 904, New Haven, Connecticut 06504

District of Delaware

4311 U.S. Courthouse, 844 King Street, Wilmington, Delaware 19801

District of Columbia

1103 U.S. Courthouse, 3rd & Constitution Avenue, NW, Washington, DC 20001

District of Columbia Superior Court

Superior Courthouse, 500 Indiana Avenue, NW, Room C-250, Washington, DC 20001

Northern Florida

PO Box 10229, Tallahassee, Florida 32302

Middle Florida

PO Box 2907, Tampa, Florida 33601-2907

Southern Florida

205 Federal Courthouse Square, 301 North Miami Avenue, Miami, Florida 33218-7785

Northern Georgia

1669 Federal Building, 75 Spring Street, SW, Atlanta, Georgia 30303

Middle Georgia

PO Box 7, Macon, Georgia 31202

Southern Georgia

PO Box 9765, Savannah, Georgia 31412

District of Guam

507 Pacific News Building, 238 Archbishop Flores Street, Agana, Guam 96910

District of Hawaii

PO Box 50184, Honolulu, Hawaii 96850

District of Idaho

741 U.S. Courthouse, 550 West Fort Street, Boise, Idaho 83724

Northern Illinois

219 S. Dearborn Street, Room 2444, Chicago, Illinois 60604

Southern Illinois

127 U.S. Courthouse, 750 Missouri Avenue, East St. Louis, Illinois 62201

Central Illinois

PO Box 156, Springfield, Illinois 62705

Northern Indiana

233 Federal Building, 204 South Main Street, South Bend, Indiana 46624

Southern Indiana

PO Box 44803, Indianapolis, Indiana 46244

Northern Iowa

320 Federal Building, 101 1st Street SE, Cedar Rapids, Iowa 52401

Southern Iowa

208 U.S. Courthouse, East First & Walnut Streets, Des Moines, Iowa 50309

District of Kansas

456 Federal Building, 444 Southeast Quincy, Topeka, Kansas 66683

Eastern Kentucky

PO Box 30, Lexington, Kentucky 40501

Western Kentucky

114 U.S. Courthouse, 601 West Broadway, Louisville, Kentucky 40202

Eastern Louisiana

C-600 U.S. Courthouse, 500 Camp Street, New Orleans, Louisiana 70130

Middle Louisiana

PO Box 3653, Baton Rouge, Louisiana 70821

Western Louisiana

PO Box 53, Shreveport, Louisiana 71161-0053

District of Maine

PO Box 349 DTS, Portland, Maine 04112

District of The Northern Mariana Islands

PO Box 570, Susupe, Saipan 96950

District of Maryland

605 U.S. Courthouse, 101 West Lombard Street, Baltimore, Maryland 21201

District of Massachusetts

PO Box 352, Boston, Massachusetts 02101

Eastern Michigan

120 Federal Building, 231 West Lafayette Street, Detroit, Michigan 48226

Western Michigan

514 Federal Building, 110 Michigan Avenue, Grand Rapids, Michigan 49503

District of Minnesota

523 U.S. Courthouse, 110 South 4th Street, Minneapolis, Minnesota 55401

Northern Mississippi

PO Box 887, Oxford, Mississippi 38655

Southern Mississippi

PO Box 959, Jackson, Mississippi 39205

Eastern Missouri

108 U.S. Courthouse, 1114 Market Street, St. Louis, Missouri 63101

Western Missouri

509 U.S. Courthouse, 811 Grand Avenue, Kansas City, Missouri 64106

District of Montana

5110 Federal Building, 316 North 26th Street, Billings, Montana 59101–1362

District of Nebraska

PO Box 1477, Omaha, Nebraska 68101

District of Nevada

PO Box 16039, Las Vegas, Nevada 89101

District of New Hampshire

PO Box 1435, Concord, New Hampshire 03302

District of New Jersey

PO Box 186, Newark, New Jersey 07101

District of New Mexico

PO Box 444, Albuquerque, New Mexico 87103

Northern New York

213 Federal Building, 10 Broad Street, Utica, New York 13501

Eastern New York

172 U.S. Courthouse, 225 Cadman Plaza East, Brooklyn, New York 11201

Southern New York

114 U.S. Courthouse Annex, 1 St. Andrew's Plaza, New York, New York 10007

Western New York

129 U.S. Courthouse, 68 Court Street, Buffalo, New York 14202

Eastern North Carolina

PO Box 25640, Raleigh, North Carolina 27611

Middle North Carolina

PO Box 1528, Greensboro, North Carolina 27402

Western North Carolina

PO Box 710, Asheville, North Carolina 28802

District of North Dakota

PO Box 2425, Fargo, North Dakota 58108–2425

Northern Ohio

B–1 U.S. Courthouse, 201 Superior Avenue, Cleveland, Ohio 44114

Southern Ohio

PO Box 688, Cincinnati, Ohio 45201

Northern Oklahoma

PO Box 1097, Tulsa, Oklahoma 74101

Eastern Oklahoma

PO Box 738, Muskogee, Oklahoma 74402

Western Oklahoma

PO Box 886, Oklahoma City, Oklahoma 73101

District of Oregon

420 U.S. Courthouse, 620 Southeast Main Street, Portland, Oregon 97205–3087

Eastern Pennsylvania

2110 U.S. Courthouse, 601 Market Street, Philadelphia, Pennsylvania 19106

Middle Pennsylvania

PO Box 310, Scranton, Pennsylvania 18501

Western Pennsylvania

539 U.S. Courthouse, 7th & Grant Streets, Pittsburgh, Pennsylvania 15219

District of Puerto Rico

PO Box 3748, San Juan, Puerto Rico 00904

District of Rhode Island

PO Box 1524, Providence, Rhode Island 02901

District of South Carolina

PO Box 1774, Columbia, South Carolina 29202

District of South Dakota

PO Box 1193, Sioux Falls, South Dakota 57101

Eastern Tennessee

PO Box 551, Knoxville, Tennessee 37901

Middle Tennessee

866 U.S. Courthouse, 801 Broadway, Nashville, Tennessee 37203

Western Tennessee

1029 Federal Building, 167 North Main Street, Memphis, Tennessee 38103

Northern Texas

1100 Commerce Street, 16F47 Federal Building, Dallas, Texas 75242

Eastern Texas

PO Box 299, Tyler, Texas 75710

Southern Texas

PO Box 61608, Houston, Texas 77208

Western Texas

235 U.S. Courthouse, 655 East Durango Boulevard, San Antonio, Texas 78206

District of Utah

PO Box 1234, Salt Lake City, Utah 84110

District of Vermont

621 Federal Building, Elmwood Avenue & Pearl Street, Burlington, Vermont 05402

Eastern Virginia

104 Federal Building, PO Box 20227–22320, 200 South Washington Street, Alexandria,
22312

Western Virginia

PO Box 2280, Roanoke, Virginia 24009

District of the Virgin Islands

PO Box 9018, St. Thomas, Virgin Islands 00801

Eastern Washington

PO Box 1463, Spokane, Washington 99210

Western Washington

300 U.S. Courthouse, 1010 5th Avenue, Seattle, Washington 98104–1188

Northern West Virginia

PO Box 1454, Elkins, West Virginia 26241

Southern West Virginia

PO Box 2667, Charleston, West Virginia 25330

Eastern Wisconsin

310 Federal Building, 517 East Wisconsin Avenue, Milwaukee, Wisconsin 53202

Western Wisconsin

440 Federal Courthouse, 120 N. Henry Street, Madison, Wisconsin 53703–2559

District of Wyoming

PO Box 768, Cheyenne, Wyoming 82003

[\[TOP\]](#)

United States Trustees

JUSTICE/UST-001

SYSTEM NAME:

Bankruptcy Case Files and Associated Records.

SECURITY CLASSIFICATION:

Sensitive But Unclassified.

SYSTEM LOCATION:

The Executive Office for United States Trustees (EOUST) and other offices of the United States Trustee Program (USTP) depending upon the judicial district where a bankruptcy case proceeding is pending or was administered. (Office addresses can be located on the Internet at <http://www.usdoj.gov/ust>.)

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals and entities involved in cases or proceedings under the Bankruptcy Code (11 U.S.C. 101, *et seq.*), including, but not limited to: debtors; creditors; bankruptcy trustee; parties in interest; professionals, attorneys, and agents representing debtors, creditors, trustees; credit counselors; debtor education providers; auditors; examiners; ombudsmen; individuals who may be considered for appointment as trustees, examiners, and ombudsmen or otherwise involved in bankruptcy cases or proceedings.

Individuals who have filed complaints, inquiries, or comments related to a bankruptcy case with the USTP.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system may include: (a) Petitions/orders for relief; (b) schedules of assets and liabilities of debtors; (c) lists of creditors; (d) statements of financial affairs; (e) operating status reports; (f) alphabetical cross-reference index cards; (g) general correspondence regarding bankruptcy cases and proceedings; (h) miscellaneous investigative records; (i) copies of certain pleadings, official forms, or other papers filed in court, including those filed with the USTP; (j) appraisal reports; (k) names of bank depositories and amounts of funds

deposited therein; (l) names of sureties and amounts of trustees' bonds; (m) tape or other recordings of creditors meetings conducted under 11 U.S.C. 341 for the purpose of examination of debtors by creditors, trustees, and others; (n) plans filed under chapter 11 or 13; (o) names of persons serving as counsel, trustee, professionals, or other functionaries in bankruptcy cases and proceedings, including compensation earned or sought by each; (p) names and qualifications of individuals who may be considered for appointment as trustee, examiners, and ombudsmen; (q) names and contact information of credit counselors and debtor education providers; (r) credit counseling certificates, debtor education certificate numbers, completion dates of credit counseling briefings and debtor education courses; (s) debt management plans; (t) means test review forms; (u) targeted and random debtor audit forms, audit reports, and related working papers; (v) federal and state tax returns; and (w) other case-related information, such as case number, case status, case type, party names and other personal identifiers, Social Security numbers and financial account numbers, estate assets/liabilities, case filings/reports, trustee bonds, calendars of meetings and hearings, due dates of plan, schedules and other filings, creditors' committee status, attorneys/professionals' data, and trustees/examiners' data, and ombudsmen data, including health care and medical records of patients of entities involved in cases or proceedings under 11 U.S.C. 101, *et seq.* and related information.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

This system is established and maintained pursuant to the bankruptcy oversight and reorganization responsibilities of the USTP under, *e.g.*, 28 U.S.C. 581, *et seq.*, and 11 U.S.C. 101, *et seq.*

PURPOSES:

The records in this system are used by USTP personnel to determine the existence of a case, to ascertain the status of actions with respect to a case, to ensure that timely action is taken, to determine the involvement by agents or other representatives of parties in cases, to implement and monitor compliance with credit counseling and debtor education requirements, and to facilitate the performance of USTP duties under, *e.g.*, 28 U.S.C. 581, *et seq.*, 11 U.S.C. 101, *et seq.*, and other legal authority.

As provided in 11 U.S.C. 107, a document filed in a case and the dockets of the bankruptcy court are public records and open to examination except when the court enters a protective order or otherwise acts to seal a docket entry.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

(A) Release of Information to Former Employees:

The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee, may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(B) Release of Information to Contractors:

Information from these records may be disclosed to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system of records.

(C) Release of Information in Proceedings:

Information from these records may be disclosed in an appropriate proceeding before a court or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before a court or administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(D) Release of Information for Litigation-related Discussions:

Information from these records may be disclosed to an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.

(E) Release of Information to Bankruptcy Trustees:

Information from these records may be disclosed to a trustee under chapter 7, 11, 12, or title 11, U.S. Code, when the United States Trustee determines that the release of such information is necessary to enable the trustee to properly administer a case or to perform duties and responsibilities of a case trustee under 28 U.S.C. 586, 18 U.S.C. 3057, or 11 U.S.C. 101, *et seq.*, including responding to complaints and inquiries related to a bankruptcy case submitted to the USTP by interested parties.

(F) Release of Information to Complainants and Victims:

Information from these records may be disclosed to complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the process and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

(G) Release of Information to the News Media:

Information from these records may be disclosed to the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(H) Release of Information to Members of Congress:

Information from these records may be disclosed to a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information on behalf of, or at the request of, the individual who is the subject of the record.

(I) Release of Information to National Archives and Records Administration:

A record from this system of records may be disclosed to the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(J) Release of Information to Law Enforcement or Regulatory Agencies:

With respect to non-law enforcement records, where a record, either alone or in conjunction

with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, tribal, or foreign law enforcement authority or other appropriate entity charged with responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

(K) Release of Information to Licensing Agencies:

Information from these records may be disclosed to federal, state, local, tribal, foreign or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

(L) Release of Information for Employment, Clearance, Contract, or Grant Purposes:

Information from these records may be disclosed to appropriate officials and employees of a Federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract, or the issuance of a grant or benefit.

(M) Release of Information to Credit/Consumer Reporting Agencies:

Information from these records may be disclosed to a credit or consumer reporting agency if such terms are used in the Fair Credit Reporting Act (15 U.S.C. 1681, *et seq.*) and the Fair Debt Collection Act (31 U.S.C. 3701, *et seq.*) when such information is necessary or appropriate to ensure that bankruptcy-related credit information is correct and accurate.

(N) Release of Information related to Investigations and Proceedings:

Information from these records may be disclosed in the course of investigating the potential actual violation of any law—whether civil, criminal, or regulatory in nature—or for the preparation of a trial or hearing for such violation. Such information may be disclosed to a Federal, state, local, tribal, or foreign agency, or to an individual or organization, if there is a reason to believe that such agency, individual, or organization possesses information relevant to the investigation, trial, or hearing, and if the dissemination is reasonably necessary to obtain such information or to obtain the cooperation of a witness or an informant.

(O) Release of Information in connection with Section 341 Meetings:

Information from these records may be disclosed in connection with meetings held under U.S.C. 341 and related proceedings, when the Department of Justice determines that the records are arguably relevant to such meetings or bankruptcy proceedings. Transcripts and other records of such meetings may also be disclosed upon request pursuant to relevant bankruptcy laws or rules.

(P) Release of Information to Law Enforcement Authority:

With respect to law enforcement records, to any criminal, civil, or regulatory law enforcement authority (whether federal, state, local, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

(Q) Release of Information to USTP Approved Credit Counseling and Debtor Education Providers:

Information from these records may be disclosed to a USTP approved credit counseling or debtor education provider when the EOUST or United States Trustee determines that the release of such information is necessary to enable the approved provider to properly perform the duties and responsibilities of a credit counseling and/or debtor education provider under U.S.C. 101, *et seq.*, and other legal authority, including responding to complaints and inquiries related to the provider, submitted to the USTP by interested parties.

(R) Release of Information to Bankruptcy Examiners:

Information from these records may be disclosed to a bankruptcy examiner appointed under title 11, U.S. Code, when the United States Trustee determines that the release of such information is necessary to enable the bankruptcy examiner to properly perform the duties and responsibilities of an examiner under 11 U.S.C. 101, *et seq.*, and other legal authority, including responding to complaints and inquiries related to a bankruptcy case, submitted to the USTP by interested parties.

(S) Release of Information to Ombudsmen:

Information from these records may be disclosed to an ombudsman appointed in a case

title 11, U.S. Code, when the United States Trustee determines that the release of such information is necessary to enable the ombudsman to properly perform the duties and responsibilities of an ombudsman under 11 U.S.C. 101, *et seq.*, and other legal authority including responding to complaints and inquiries related to a bankruptcy case, submit the USTP by interested parties.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system, except as specified below, are recorded on paper/cardboard media and maintained in file cabinets, storage containers, electric file/card retrievers, or safes. Records in this system are entered into automated information systems and stored on semiconductor and/or magnetic disks for use or reproduction in report form at various times.

RETRIEVABILITY:

In USTP field offices, bankruptcy case records are retrieved by bankruptcy court case numbers, cross-referenced alphabetically by names of debtors. Bankruptcy case records pertaining to case trustees, sureties, depository banks, and to agents representing parties are maintained and retrieved alphabetically. Bankruptcy case records and records of potential candidates for appointment as trustees, examiners, and ombudsmen in the EOUST are maintained and retrieved alphabetically by name of the debtor or the particular person involved. Automated information is retrieved by a variety of key words, including names of individuals.

SAFEGUARDS:

Records contained in this system are unclassified. They are safeguarded and protected in accordance with Departmental rules and procedures governing the handling of office records and computerized information. During duty hours, access to this system is monitored and controlled by USTP personnel. During nonduty hours, offices are locked.

RETENTION AND DISPOSAL:

Chapter 7 no-asset case records may be destroyed six months after the case is closed.

341 meeting tapes may be destroyed two years after the date of the 341 meeting. Chapter 11 case records may be destroyed three years after the case is closed. Chapter 12 case records may be destroyed three years after the case is dismissed or closed. Chapter 13 case records may be destroyed six months after the case is dismissed or closed. To prevent unauthorized disclosure, records are destroyed by shredding, burning, or similar methods.

SYSTEM MANAGER(S) AND ADDRESS:

The system managers for this system of records are: (a) the United States Trustees or Assistant United States Trustees, to the extent these records are maintained in their offices and (b) the General Counsel, to the extent these records are maintained in the EOUST. Addresses can be located on the Internet at <http://www.usdoj.gov/ust>.)

NOTIFICATION PROCEDURE:

Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the address listed on the USTP FOIA/Privacy Act Web site (<http://www.usdoj.gov/ust>). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.40, *et seq.*

RECORD ACCESS PROCEDURES:

Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the address listed on the USTP FOIA/Privacy Act Web site (<http://www.usdoj.gov/ust>). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.40, *et seq.*

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should clearly and concisely state what information is being contested, the reasons for contesting it, and the proposed amendment to the information. Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the address listed on the USTP FOIA/Privacy Act Web site (<http://www.usdoj.gov/ust>). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.40, *et seq.*

RECORD SOURCE CATEGORIES:

Sources of information contained in this system generally consist of debtors, creditors, trustees, examiners, auditors, ombudsmen, USTP approved credit counseling and/or debt education providers, attorneys, and other agents participating in the administration of a judges of the bankruptcy courts and other judicial officers, parties in interest, and employees of the USTP.

EXEMPTIONS CLAIMED FOR SYSTEM:

None.

[\[TOP\]](#)

JUSTICE/UST-002

SYSTEM NAME:

Bankruptcy Trustee Oversight Records

SECURITY CLASSIFICATION:

Sensitive But Unclassified

SYSTEM LOCATION:

The Executive Office for United States Trustees (EOUST) and other offices of the United States Trustee Program (USTP) depending upon the judicial district where the bankruptcy case trustee serves or has made application to serve. (Office addresses can be located on the Internet at <http://www.usdoj.gov/ust>.)

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Persons serving or applying to serve as estate trustees in bankruptcy cases filed under 7, 11, 12, or 13 of the Bankruptcy Code (11 U.S.C. 101, *et seq.*) and/or subject to USTP oversight pursuant to 28 U.S.C. 586.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system may include: resumes, applications, references, recommendation related materials; notes, correspondence, memoranda, messages, and agreements; audits, reviews, evaluations, financial records, transcripts, and security clearance information; Social Security numbers, financial account numbers, and other personal identifiers; and other information provided to USTP by trustees, applicants, and third parties or developed by personnel.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

This system is established and maintained pursuant to the bankruptcy oversight and responsibilities of the USTP under, *e.g.*, 28 U.S.C. 581, *et seq.*, and 11 U.S.C. 101, *et seq.*

PURPOSE:

These records are used by USTP personnel for determining and reassessing the qualifications and eligibility of persons serving or applying to serve as trustees in bankruptcy cases.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:***(A) Release of Information to Former Employees:***

The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee, if necessary, for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(B) Release of Information to Contractors:

Information from these records may be disclosed to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative

agreement, or other assignment for the federal government, when necessary to accomplish agency function related to this system of records.

(C) Release of Information in Proceedings:

Information from these records may be disclosed in an appropriate proceeding before a court or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(D) Release of Information for Litigation-related Discussions:

Information from these records may be disclosed to an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.

(E) Release of Information to Bankruptcy Trustees:

Information from these records may be disclosed to a trustee under chapter 7, 11, 12, or 13 of title 11, U.S. Code, when the United States Trustee determines that the release of such information is necessary to enable the trustee to properly administer a case or to perform the duties and responsibilities of a case trustee under 28 U.S.C. 586, 18 U.S.C. 3057, or 11 U.S.C. 1101, *et seq.*, including responding to complaints and inquiries related to a bankruptcy case submitted to the USTP by interested parties.

(F) Release of Information to Complainants and Victims:

Information from these records may be disclosed to complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the process and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

(G) Release of Information to the News Media:

Information from these records may be disclosed to the news media and the public, including

disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(H) Release of Information to Members of Congress:

Information from these records may be disclosed to a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information on behalf of, or at the request of, the individual who is the subject of the record.

(I) Release of Information to National Archives and Records Administration:

A record from this system of records may be disclosed to the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(J) Release of Information to Law Enforcement or Regulatory Agencies:

With respect to non-law enforcement records, where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

(K) Release of Information to Licensing Agencies:

Information from these records may be disclosed to federal, state, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

(L) Release of Information to Credit/Consumer Reporting Agencies:

Information from these records may be disclosed to a credit or consumer reporting agency when such terms are used in the Fair Credit Reporting Act (15 U.S.C. 1681, *et seq.*) and the Fair Debt Collection Act (31 U.S.C. 3701, *et seq.*), when such information is necessary or appropriate.

ensure that bankruptcy-related credit information is correct and accurate.

(M) Release of Information Related to Investigations and Proceedings:

Information from these records may be disclosed in the course of investigating the potential actual violation of any law—whether civil, criminal, or regulatory in nature—or for the preparation of a trial or hearing for such violation. Such information may be disclosed to federal, state, local, tribal, or foreign agency, or to an individual or organization, if there is reason to believe that such agency, individual, or organization possesses information relevant to the investigation, trial, or hearing, and if the dissemination is reasonably necessary to obtain such information or to obtain the cooperation of a witness or an informant.

(N) Release of Information in Connection with Section 341 Meetings:

Information from these records may be disclosed in connection with meetings held under U.S.C. 341 and related proceedings when the Department of Justice determines that the records are arguably relevant to such meetings or proceedings. Transcripts or other records of such meetings may also be disclosed upon request pursuant to relevant bankruptcy law rules.

(O) Release of Information to Law Enforcement Authority

With respect to law enforcement records, to any criminal, civil, or regulatory law enforcement authority (whether federal, state, local, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system, except as specified below, are recorded on paper/cardboard media and maintained in file cabinets, storage containers, electric file/card retrievers, or safes. Electronic records in this system are entered into automated information systems and stored on semiconductor and/or magnetic disks for use or reproduction in report form at various times.

RETRIEVABILITY:

In USTP field offices, bankruptcy trustee oversight records are filed alphabetically by the trustee's or applicant's name. In EOUST, similar records are maintained alphabetically, organized by region. Automated information is retrieved by a variety of key words, including names of individuals.

SAFEGUARDS:

Records contained in this system are unclassified. They are safeguarded and protected in accordance with Departmental rules and procedures governing the handling of official records and computerized information. During duty hours, access to this system is monitored and controlled by USTP office personnel. During nonduty hours, offices are locked.

RETENTION AND DISPOSAL:

Bankruptcy trustee oversight records may be destroyed after three years except in the following circumstances. If the trustee dies, his/her trustee oversight records may be destroyed after one year. Case Trustee Interim Reports may be destroyed after five years. To prevent unauthorized disclosure, records are destroyed by shredding, burning, or similar methods.

SYSTEM MANAGER(S) AND ADDRESS:

The system managers for this system of records are: (a) the United States Trustees or Assistant United States Trustees, to the extent these records are maintained in their offices and (b) the Assistant Director, Office of Review and Oversight, to the extent these records are maintained in the EOUST. (Office addresses can be located on the Internet at <http://www.usdoj.gov/ust>.)

NOTIFICATION PROCEDURE:

Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the address listed on the USTP FOIA/Privacy Act Web site (<http://www.usdoj.gov/ust>). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 U.S.C. 16.40, *et seq.*

RECORD ACCESS PROCEDURE:

Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the

address listed on the USTP FOIA/Privacy Act Web site &fnl;(http://www.usdoj.gov/ust). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.40, *et seq.*

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should clearly and concisely state what information is being contested, the reasons for contesting it, and the proposed amendment to the information. Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the address listed on the USTP FOIA/Privacy Act Web site (http://www.usdoj.gov/ust). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.40, *et seq.*

RECORD SOURCE CATEGORIES:

Sources of information contained in this system generally consist of the applicant, the applicant's references, interested third parties, and/or USTP personnel.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[\[TOP\]](#)

JUSTICE/UST-003

SYSTEM NAME:

U.S. Trustee Program Timekeeping Records.

SECURITY CLASSIFICATION:

Sensitive But Unclassified.

SYSTEM LOCATION:

The Executive Office for United States Trustees (EOUST) and other offices of the United States Trustee Program.

Trustee Program (USTP) depending upon where an employee has been assigned for duty. (Office addresses can be located on the Internet at <http://www.usdoj.gov/ust>.)

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Employees of the USTP field offices, generally to include Assistant United States Trustee attorneys, bankruptcy analysts, paralegal specialists, and clerical support staff.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system may include USTP employees' names, personal identifiers, and record of their work time.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

This system is established and maintained pursuant to the responsibilities of the USTP e.g., 28 U.S.C. 581, *et seq.*, and 11 U.S.C. 101, *et seq.*

PURPOSE:

This system consists of records of the work time of employees of the USTP, and is used to evaluate workload as a basis for requesting and allocating personnel and other resources.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

(A) Release of Information to Former Employees:

The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(B) Release of Information to Contractors:

Information from these records may be disclosed to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system of records.

(C) Release of Information to Members of Congress:

Information from these records may be disclosed to a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information on behalf of, or at the request of, the individual who is the subject of the record.

(D) Release of Information to National Archives and Records Administration:

A record from this system of records may be disclosed to the National Archives and Records Administration for the purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(E) Release of Information in Proceedings:

Information from these records may be disclosed in an appropriate proceeding before a court or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before a court or administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

(F) Release of Information related to Investigations and Proceedings:

Information from these records may be disclosed in the course of investigating the potential actual violation of any law—whether civil, criminal, or regulatory in nature—or for the preparation of a trial or hearing for such violation. Such information may be disclosed to a federal, state, local, tribal, or foreign agency, or to an individual or organization, if there is a reason to believe that such agency, individual, or organization possesses information relevant to the investigation, trial, or hearing, and if the dissemination is reasonably necessary to obtain such information or to obtain the cooperation of a witness or an informant.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING,

DISPOSING OF RECORDS IN THE SYSTEM:***STORAGE:***

Records in this system, except as specified below, are recorded on paper/cardboard media and maintained in file cabinets, storage containers, electric file/card retrievers, or safes. Records in this system are entered into automated information systems and stored on semiconductor and/or magnetic disks for use or reproduction in report form at various times.

RETRIEVABILITY:

In USTP field offices, USTP timekeeping records are maintained by the name of the employee. In EOUST, such records are maintained and organized by USTP office, job title, and the name of the employee. Automated information is retrieved by a variety of key words.

SAFEGUARDS:

Records contained in this system are unclassified. They are safeguarded and protected in accordance with Departmental rules and procedures governing the handling of official records and computerized information. During duty hours, access to this system is monitored and controlled by USTP office personnel. During nonduty hours, offices are locked.

RETENTION AND DISPOSAL:

These records may be destroyed by shredding, burning, or similar methods after being reviewed or when three years old.

SYSTEM MANAGER(S) AND ADDRESS:

The system managers for this system of records are: (a) the United States Trustees or Assistant United States Trustees, to the extent these records are maintained in their offices and (b) the Assistant Director, Office of Research and Planning, to the extent these records are maintained in the EOUST. (Office addresses can be located on the Internet at <http://www.usdoj.gov/ust>.)

NOTIFICATION PROCEDURE:

Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at 1

address listed on the USTP FOIA/Privacy Act Web site &fml;(http://www.usdoj.gov/ust). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.40, *et seq.*

RECORD ACCESS PROCEDURE:

Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the address listed on the USTP FOIA/Privacy Act Web site &fml;(http://www.usdoj.gov/ust). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.40, *et seq.*

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should clearly and concisely state what information is being contested, the reasons for contesting it, and the proposed amendment to the information. Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the address listed on the USTP FOIA/Privacy Act Web site (http://www.usdoj.gov/ust). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.40, *et seq.*

RECORD SOURCE CATEGORIES:

Sources of information contained in this system generally consist of USTP personnel.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[\[TOP\]](#)

JUSTICE/UST-004

SYSTEM NAME:

U.S. Trustee Program Case Referral System.

SECURITY CLASSIFICATION:

Sensitive But Unclassified.

SYSTEM LOCATION:

The Executive Office for United States Trustees (EOUST) and other offices of the United States Trustee Program (USTP), depending on where the acts under investigation occurred. (Court addresses can be located on the Internet at <http://www.usdoj.gov/ust>.)

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Entities and individuals involved in the bankruptcy process who are suspected of having engaged in criminal conduct or of having violated other federal laws, and whose activities have been or may be investigated or reported by the USTP to a United States Attorney or other law enforcement authority for investigation, prosecution, or other action pursuant to 28 U.S.C. 18 U.S.C. 3057, or other legal authority.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system may include information associated with a referral to law enforcement authorities in connection with bankruptcy proceedings or related matters arising under 18 U.S.C. 101, *et seq.*, or 28 U.S.C. 581, *et seq.* This system may contain information pertaining to the subject of the referral, who may be a debtor, creditor, party in interest, credit counselor and/or debtor education provider, or any other entity associated with the bankruptcy or proceedings. This system may also contain information about the proceedings with which the subject of the referral is associated. Such information may include the subject's name, address, date of birth, Social Security number, financial account numbers, or other personal identifiers; a chronological account of the incident(s); the source of the information, including confidential sources, if any; witnesses' names, addresses, and other personal identifiers; the law enforcement agency to which the referral is made; the status or final disposition of the referral; the case number, chapter, and status of any related proceedings; the bankruptcy trustee/examiner's name, address, phone number, and other personal identifiers; the judge assigned to the case; and such other case data as may be furnished to or available in the records of the court or of the USTP.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

This system is established and maintained pursuant to the responsibilities of the USTP

e.g., 28 U.S.C. 581, *et seq.*, 11 U.S.C. 101, *et seq.*, and 18 U.S.C. 3057.

PURPOSE(S):

The purposes of this system are to assist the United States Trustees: (1) in supervising administration of cases and trustees in cases and proceedings filed under the Bankrupt Code (11 U.S.C. 101, *et seq.*); (2) in carrying out their congressional mandate "to serve bankruptcy watch-dogs to prevent fraud, dishonesty, and overreaching in the bankrupt arena" (H.R. Rep. No. 595, 95th Cong., 2d Sess. 88 (1978)); and (3) in complying with 18 U.S.C. 3057, which directs trustees to report for investigation any instance where there are reasonable grounds for believing that there has been a violation of federal laws relating to insolvent debtors or reorganization plans. The USTP may inform the appropriate law enforcement authorities when fraud or other violations of federal law are suspected or discovered in a bankruptcy case and will maintain records thereof described under "Categories of Records in the System" (above). The data will be used for Program-wide evaluation purposes, for statistical purposes, and to track the number, type, and outcome of cases referred for investigation.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

(A) Release of Information to Former Employees:

The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee, if necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(B) Release of Information to Contractors:

Information from these records may be disclosed to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish an agency function related to this system of records.

(C) Release of Information in Proceedings:

Information from these records may be disclosed in an appropriate proceeding before a court or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator holds the records to be relevant to the proceeding.

(D) Release of Information for Litigation-related Discussions:

Information from these records may be disclosed to an actual or potential party to litigation or to the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.

(E) Release of Information to Bankruptcy Trustees:

Information from these records may be disclosed to a trustee under chapter 7, 11, 12, or 13 of title 11, U.S. Code, when the United States Trustee determines that the release of such information is necessary to enable the trustee to properly administer a case or to perform the duties and responsibilities of a case trustee under 28 U.S.C. 586, 18 U.S.C. 3057, or 11 U.S.C. 101, *et seq.*, including responding to complaints and inquiries related to a bankruptcy case submitted to the USTP by interested parties.

(F) Release of Information to Complainants and Victims:

Information from these records may be disclosed to complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the process and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

(G) Release of Information to the News Media:

Information from these records may be disclosed to the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of privacy.

(H) Release of Information to Members of Congress:

Information from these records may be disclosed to a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information on behalf of, or at the request of, the individual to whom the records pertain.

(I) Release of Information to National Archives and Records Administration:

These records may be disclosed to the National Archives and Records Administration for the purposes of records management inspections conducted under the authority of 44 U.S.C. 2906.

(J) Release of Information to Law Enforcement or Regulatory Agencies:

With respect to non-law enforcement records, where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, tribal, or foreign law enforcement authority or other appropriate entity charged with responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

(K) Release of Information to Licensing Agencies:

Information from these records may be disclosed to federal, state, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

(L) Release of Information to Judicial Branch:

These records may be disclosed to members of the judicial branch of the federal government where disclosure appears relevant to the authorized function of the recipient judicial officer or court system under 18 U.S.C. 3057.

(M) Release of Information to Credit/Consumer Reporting Agencies:

Information from these records may be disclosed to a credit or consumer reporting agency.

such terms are used in the Fair Credit Reporting Act (15 U.S.C. 1681, *et seq.*) and the Fair Debt Collection Act (31 U.S.C. 3701, *et seq.*), when such information is necessary or appropriate to ensure that bankruptcy-related credit information is correct and accurate.

(N) Release of Information Related to Investigations and Proceedings:

Information from these records may be disclosed in the course of investigating the potential actual violation of any law—whether civil, criminal, or regulatory in nature—or for the preparation of a trial or hearing for such violation. Such information may be disclosed to federal, state, local, tribal, or foreign agency, or to an individual or organization, if there is a reasonable basis to believe that such agency, individual, or organization possesses information relevant to the investigation, trial, or hearing, and if the dissemination is reasonably necessary to obtain such information or to obtain the cooperation of a witness or an informant.

(O) Release of Information in Connection with Section 341 Meetings:

Information from these records may be disclosed in connection with meetings held under 11 U.S.C. 341 and related proceedings, when the Department of Justice determines that the records are arguably relevant to such meetings or proceedings. Transcripts or other records of such meetings may also be disclosed upon request pursuant to relevant bankruptcy law rules.

(P) Release of Information to Law Enforcement Authority:

With respect to law enforcement records, to any criminal, civil, or regulatory law enforcement authority (whether federal, state, local, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

(Q) Release of Information to USTP Approved Credit Counseling and Debtor Education Providers:

Information from these records may be disclosed to a USTP approved credit counseling or debtor education provider when the EOUST or United States Trustee determines that the release of such information is necessary to enable the approved provider to properly perform the duties and responsibilities of a credit counseling and/or debtor education provider under 11 U.S.C. 101, *et seq.*, and other legal authority, including responding to complaints and inquiries.

related to the provider, submitted to the USTP by interested parties.

(R) Release of Information to Bankruptcy Examiners:

Information from these records may be disclosed to a bankruptcy examiner appointed in a case under title 11, U.S. Code, when the United States Trustee determines that the release of such information is necessary to enable the bankruptcy examiner to properly perform the duties and responsibilities of an examiner under 11 U.S.C. 101, *et seq.*, and other legal authority, including responding to complaints and inquiries related to a bankruptcy case, submitted to the USTP by interested parties.

(S) Release of Information to Ombudsmen:

Information from these records may be disclosed to an ombudsman appointed in a case under title 11, U.S. Code, when the United States Trustee determines that the release of such information is necessary to enable the ombudsman to properly perform the duties and responsibilities of an ombudsman under 11 U.S.C. 101, *et seq.*, and other legal authority, including responding to complaints and inquiries related to a bankruptcy case, submitted to the USTP by interested parties.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system, except as specified below, are recorded on paper/cardboard media and maintained in file cabinets, storage containers, electric file/card retrievers, or safes. Records in this system are entered into automated information systems and stored on semiconductor and/or magnetic disks for use or reproduction in report form at various times.

RETRIEVABILITY:

In EOUST and in USTP field offices, case referral records are filed alphanumerically or chronologically. Automated information is retrieved by a variety of key words, including names of individuals or other personal identifiers.

SAFEGUARDS:

Records contained in this system are unclassified but highly sensitive. They are safeguarded and protected in accordance with Departmental rules and procedures governing the handling of official records and computerized information. During duty hours, access to this system is monitored and controlled by USTP office personnel. During nonduty hours, access is limited. Only those persons with a need to know have access to the records.

RETENTION AND DISPOSAL:

Criminal referral records may be destroyed by shredding, burning, or similar methods five years from the date of the finding of insufficient evidence, declination of prosecution, or voting of a No True Bill by a Grand Jury. For criminal referral records in which criminal cases have been brought, such records may be destroyed five years from the date of sentencing or the date of a nonappealable judicial determination, whichever is later (National Archives and Records Administration approval pending).

SYSTEM MANAGER(S) AND ADDRESS:

The system managers for this system of records are: (a) the United States Trustees or Assistant United States Trustees, to the extent these records are maintained in their offices and (b) Office of the General Counsel and/or Chief of Criminal Enforcement, to the extent these records are maintained in the EOUST. (Office addresses can be located on the Internet at <http://www.usdoj.gov/ust>.)

NOTIFICATION PROCEDURE:

Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the address listed on the USTP FOIA/Privacy Act Web site (<http://www.usdoj.gov/ust>). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.40, *et seq.*

RECORDS ACCESS PROCEDURE:

Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the address listed on the USTP FOIA/Privacy Act Web site (<http://www.usdoj.gov/ust>). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.40, *et seq.*

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should clearly and concisely state what information is being contested, the reasons for contesting it, and a proposed amendment to the information. Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the address listed on the USTP FOIA/Privacy Act Worksheet (<http://www.usdoj.gov/ustp>). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.40, *et seq.*

RECORD SOURCE CATEGORIES:

The records generally contain information obtained by or furnished to the USTP from: (1) Federal or state court records; (2) debtors or debtors' principals, agents or representative informants and interested third parties; and (4) other law enforcement sources.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Attorney General has exempted this system of records from subsections (c)(3) and (e)(1), (2), and (3), (e)(4)(G) and (H), (e)(5) and (8); (f) and (g) of the Privacy Act, pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e) and have been published in the *Federal Register*. See 28 CFR 16.77.

[\[TOP\]](#)

JUSTICE/UST-005

SYSTEM NAME:

Credit Counseling and Debtor Education Files and Associated Records.

SECURITY CLASSIFICATION:

Sensitive But Unclassified

SYSTEM LOCATION:

The Executive Office for U.S. Trustees (EOUST) and other offices of the United States Trustee Program (USTP) depending upon the judicial district(s) where the credit counselor or debtor education provider delivers services or has made application to deliver services under title 11, U.S. Code (11 U.S.C. 101, *et seq.*). (Office addresses can be located on the Internet at <http://www.usdoj.gov/ust>.)

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals and entities applying for approval and reapproval by the United States Trustee(s) to provide credit counseling and/or debtor education services under title 11, U.S. Code, include, but not limited to: (a) primary contact persons, agency representatives, principals, owners, counselors, educators, teachers, sole proprietors, managers, supervisors, employees, and former directors, officers, and trustees; (b) individuals and entities whose approval or reapproval are pending or withdrawn or have been granted, denied, or revoked by the United States Trustee(s); (c) other parties in interest, agents, affiliates, related entities, independent contractors, contract service providers, credit counseling and debtor education clients, students, professionals, debtors, creditors, bankruptcy trustees, attorneys, accountants, auditors, or those otherwise involved in credit counseling and debtor education.

Individuals who have filed complaints or comments with the United States Trustee(s) or against credit counseling and debtor education providers whose approval and reapproval are pending or withdrawn or have been granted, denied, or revoked by the United States Trustee(s) under title 11, U.S. Code.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records in this system may include: (a) Applications, appendices, and related documents submitted to EOUST or the United States Trustee(s) by credit counseling agencies and education providers; (b) supplemental submissions to applications and related correspondence; (c) data relating to the agencies' and providers' approval status and performance such as memoranda, notes, messages, check lists, reviews, and evaluation information from federal, state, and local government agencies, including Internal Revenue Service (IRS) release/waiver forms and IRS audit information; (e) Social Security numbers and tax identification numbers; (f) federal and state tax returns; (g) names, addresses, business locations and corresponding judicial districts, email addresses, telephone and fax numbers, resumes, Curriculum Vitae, education, qualifications, and/or experience of primary contacts.

persons, agency representatives, principals, owners, counselors, educators, teachers, s proprietors, managers, supervisors, employees, current and former directors, officers, a trustees, parties in interest, agents, affiliates, subsidiaries, related entities, independent contractors, contract service providers, professionals, attorneys, accountants, and audit including compensation earned or sought by each; (h) names of sureties and amounts bonds, securities, insurance policies, and letters of credit; (i) general correspondence, f contracts, client agreements, schedules, budget analysis forms, training materials, cour and teaching methods, manuals, procedures, scripts, counseling materials, debtor educ curriculum, and Internet information; (j) fee schedules, suggested contributions, and "fa share" contributions made by creditors; (k) bank and financial institution information, inc names of depositories and amounts of funds deposited in operating accounts and trust accounts; (l) audits, audited and unaudited financial statements, and cash flow projectio (balance sheets, profit and loss statements, and statements of cash flow, and a year-to budget versus actual comparison, including all underlying assumptions); (m) annual disbursements; (n) business plans; (o) debt management plan servicing agreements; (p statistics and activity reports; (q) background checks and miscellaneous investigative re (r) copies of certain pleadings or other papers filed in court, including those filed by the (s) bond or other claims, arbitrations, and mediations, (t) tracking and monitoring record management reports, including information obtained during onsite visits to credit couns and debtor education providers to monitor quality assurance, such as records, notes, ar recorded client counseling sessions and debtor education courses; (u) disciplinary and enforcement actions and administrative reviews; (v) licenses, accreditations, and certific (w) standards, guidelines, and memberships with associations, (x) credit counseling certificates, debt management plans, debtor education certificates, certificate numbers, certificate issue and completion dates, and bankruptcy case names and numbers, (y) acknowledgments, agreements, and declarations; and (z) names of complainants, com complaint forms, comments, related correspondence, client surveys, client evaluations ; forms, and complaint reports and referral information, including records provided to and received from federal, state, and local agencies.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

This system is established and maintained pursuant to the bankruptcy oversight and re responsibilities of the USTP under, e.g., 28 U.S.C. 581, *et seq.*, and 11 U.S.C. 101, *et s* and other legal authority.

PURPOSES:

The records in this system will be used to assist the EOUST and United States Trustee(

- (a) Determine and reassess the suitability, eligibility, and qualifications of persons providing credit counseling and/or debtor education services under title 11, U. Code;
- (b) maintain the requisite data conveniently;
- (c) ensure compliance with statutory requirements;
- (d) monitor credit counseling agencies' and debtor education providers' status, compliance with approval standards, and performance of approved providers;
- (e) monitor the issuance of certificates and detect and deter certificate forgery; and
- (f) collect and maintain complaints and comments from bankruptcy debtors and the public in order to take appropriate actions, including referrals to other government agencies.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

(A) Release of Information to Former Employees:

The Department of Justice may disclose relevant and necessary information to a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority in accordance with applicable Department regulations; or facilitating communications with a former employee may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

(B) Release of Information to Contractors:

Information from these records may be disclosed to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government, when necessary to accomplish agency function related to this system of records.

(C) Release of Information in Proceedings:

Information from these records may be disclosed in an appropriate proceeding before a court or administrative or adjudicative body, when the Department of Justice determines that the records are arguably relevant to the proceeding; or in an appropriate proceeding before a court or administrative or adjudicative body when the adjudicator determines the records to be relevant.

to the proceeding.

(D) Release of Information for Litigation-Related Discussions:

Information from these records may be disclosed to an actual or potential party to litigate the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.

(E) Release of Information to Bankruptcy Trustees:

Information from these records may be disclosed to a trustee under chapter 7, 11, 12, or title 11, U.S. Code, when the United States Trustee determines that the release of such information is necessary to enable the trustee to properly administer a case or to perform duties and responsibilities of a case trustee under 28 U.S.C. 586, 18 U.S.C. 3057, or 11 U.S.C. 101, *et seq.*, including responding to complaints and inquiries related to a bankruptcy case submitted to the USTP by interested parties.

(F) Release of Information to Complainants and Victims:

Information from these records may be disclosed to complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the process and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.

(G) Release of Information to the News Media:

Information from these records may be disclosed to the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

(H) Release of Information to Members of Congress:

Information from these records may be disclosed to a Member of Congress or staff acting on the Member's behalf when the Member or staff requests the information on behalf of, at the request of, the individual who is the subject of the record.

(I) Release of Information to National Archives and Records Administration:

A record from this system of records may be disclosed to the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

(J) Release of Information to Law Enforcement or Regulatory Agencies:

With respect to non-law enforcement records, where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate federal, state, local, tribal, or foreign law enforcement authority or other appropriate entity charged with responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

(K) Release of Information to Licensing Agencies:

Information from these records may be disclosed to federal, state, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

(L) Release of Information for Employment, Clearance, Contract, or Grant Purposes:

Information from these records may be disclosed to appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.

(M) Release of Information to Credit/Consumer Reporting Agencies:

Information from these records may be disclosed to a credit or consumer reporting agency when such terms are used in the Fair Credit Reporting Act (15 U.S.C. 1681, *et seq.*) and the Fair Debt Collection Act (31 U.S.C. 3701, *et seq.*), when such information is necessary or appropriate to ensure that bankruptcy-related credit information is correct and accurate.

(N) Release of Information Related to Investigations and Proceedings:

Information from these records may be disclosed in the course of investigating the potential actual violation of any law—whether civil, criminal, or regulatory in nature—or for the preparation of a trial or hearing for such violation. Such information may be disclosed to federal, state, local, tribal, or foreign agency, or to an individual or organization, if there is reason to believe that such agency, individual, or organization possesses information relevant to the investigation, trial, or hearing, and if the dissemination is reasonably necessary to obtain such information or to obtain the cooperation of a witness or an informant.

(O) Release of Information in Connection with Section 341 Meetings:

Information from these records may be disclosed in connection with meetings held under U.S.C. 341 and related proceedings, when the Department of Justice determines that the records are arguably relevant to such meetings or bankruptcy proceedings. Transcripts and other records of such meetings may also be disclosed upon request pursuant to relevant bankruptcy laws or rules.

(P) Release of Information to Law Enforcement Authority

With respect to law enforcement records, to any criminal, civil, or regulatory law enforcement authority (whether federal, state, local, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities.

(Q) Release of Information in Connection with USTP Decisions to Grant, Deny, or Revoke Approval or Reapproval of Credit Counseling and Debtor Education Applicants and Providers

Information from these records may be disclosed to appropriate third parties to the extent necessary to collect or verify information pertinent to the USTP's decision to grant, deny, revoke approval or reapproval of a provider of credit counseling or debtor education services under title 11, U.S. Code, including to a federal, state, local, tribal, or foreign agency, or individual or organization, if there is reason to believe that such agency, individual, or organization possesses information that the USTP needs to make a determination relating to the granting, denial, or revocation of approval or reapproval of an applicant, and if the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of any third party.

(R) Release of Information to USTP Approved Credit Counseling and Debtor Education Providers:

Information from these records may be disclosed to a USTP approved credit counseling debtor education provider when the EOUST or United States Trustee determines that the release of such information is necessary to enable the approved provider to properly perform the duties and responsibilities of a credit counseling and/or debtor education provider under U.S.C. 101, *et seq.*, and other legal authority, including responding to complaints and inquiries related to the provider, submitted to the USTP by interested parties.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system, except as specified below, are recorded on paper/cardboard media and maintained in file cabinets, storage containers, electric file/card retrievers, or safes. Records in this system are entered into automated information systems and stored on semiconductor and/or magnetic disks for use or reproduction in report form at various times.

RETRIEVABILITY:

In EOUST, records are maintained and organized alphanumerically by assigned number and alphabetically by name. In USTP field offices, credit counseling and debtor education records are filed alphabetically by the applicant's name and assigned number. Automated information is retrieved by a variety of key words, including names of individuals and other personal identifiers.

SAFEGUARDS:

Records contained in this system are unclassified. They are safeguarded and protected in accordance with Departmental rules and procedures governing the handling of official records and computerized information. During duty hours, access to this system is monitored and controlled by USTP office personnel. During nonduty hours, offices are locked.

RETENTION AND DISPOSAL:

Credit counseling and debtor education applications and related records may be destroyed three years after the date of the USTP's final dispositive decision or final agency action or five years from the date of a nonappealable judicial determination, except in the following circumstances. If the provider dies or withdraws an initial application for a six-month appeal period before a final decision by the UST is made to approve or disapprove the application, records may be destroyed after one year. Complaints filed with the USTP may be destroyed two years from the date of receipt. To prevent unauthorized disclosure, records are destroyed by shredding, burning, or similar methods. (National Archives and Records Administration approval pending).

SYSTEM MANAGER(S) ADDRESS:

The system managers for this system of records are (a) the Chief, Credit Counseling and Debtor Education Unit, to the extent these records are maintained in the EOUST; and (b) the United States Trustee(s) or Assistant United States Trustee(s) to the extent these records are maintained in their offices. (Office addresses can be located on the Internet at <http://www.usdoj.gov/ust>).

NOTIFICATION PROCEDURE:

Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the address listed on the USTP FOIA/Privacy Act Web site &fnl;(<http://www.usdoj.gov/ust>). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 U.S.C. 16.40, *et seq.*

RECORD ACCESS PROCEDURES:

Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the address listed on the USTP FOIA/Privacy Act Web site &fnl;(<http://www.usdoj.gov/ust>). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 U.S.C. 16.40, *et seq.*

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should clearly and concisely state what information is being contested, the reason for contesting it, and

proposed amendment to the information. Address such inquiries to the Office of the General Counsel (FOIA/Privacy Counsel) at the address listed on the USTP FOIA/Privacy Act Worksheet (<http://www.usdoj.gov/ust>). The envelope and letter should be clearly marked "Privacy Act Request" and comply with 28 CFR 16.40, *et seq.*

RECORD SOURCE CATEGORIES:

Sources of information contained in this system generally consist of the credit counselor and/or debtor education provider applicants, and those whose applications for approval or reapproval have been withdrawn by the applicant or granted, denied, or revoked by the States Trustee(s); the applicants' references; interested third parties; federal and state agencies; and/or USTP personnel.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[\[TOP\]](#)

Title 28—Judicial Administration

Chapter I—Department of Justice

PART 16—PRODUCTION OR DISCLOSURE OF MATERIAL OR INFORMATION

Subpart D—Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974

16.40 General provisions.

16.41 Requests for access to records.

16.42 Responsibility for responding to requests for access to records.

16.43 Responses to requests for access to records.

16.44 Classified information.

16.45 Appeals from denials of requests for access to records.

16.46 Requests for amendment or correction of records.

16.47 Requests for an accounting of record disclosures.

16.48 Preservation of records.

16.49 Fees.

16.50 Notice of court-ordered and emergency disclosures.

16.51 Security of systems of records.

16.52 Contracts for the operation of record systems.

16.53 Use and collection of social security numbers.

16.54 Employee standards of conduct.

16.55 Other rights and services.

Subpart E—Exemption of Records Systems Under the Privacy Act

16.70 Exemption of the Office of the Attorney General System—limited access.

16.71 Exemption of the Office of the Deputy Attorney General System—limited access.

16.72 Exemption of Office of the Associate Attorney General System—limited access.

16.73 Exemption of Office of Legal Policy System—limited access.

16.74 Exemption of National Security Division Systems—limited access.

16.75 Exemption of the Office of the Inspector General Systems/Limited Access.

16.76 Exemption of Justice Management Division.

16.77 Exemption of U.S. Trustee Program System—limited access.

16.78 Exemption of the Special Counsel for Immigration-Related, Unfair Employment Practices Systems.

16.79 Exemption of Pardon Attorney System.

16.80 Exemption of Office of Professional Responsibility System—limited access.

16.81 Exemption of United States Attorneys Systems—limited access.

16.82 Exemption of the National Drug Intelligence Center Data Base—limited access.

16.83 Exemption of the Executive Office for Immigration Review System—limited access

16.84 Exemption of Immigration Appeals System.

16.85 Exemption of U.S. Parole Commission—limited access.

16.88 Exemption of Antitrust Division Systems—limited access.

16.89 Exemption of Civil Division Systems—limited access.

16.90 Exemption of Civil Rights Division Systems.

16.91 Exemption of Criminal Division Systems—limited access, as indicated.

16.92 Exemption of Environment and Natural Resources Division Systems—limited access

16.93 Exemption of Tax Division Systems—limited access.

16.96 Exemption of Federal Bureau of Investigation Systems—limited access.

16.97 Exemption of Bureau of Prisons Systems—limited access.

16.98 Exemption of the Drug Enforcement Administration (DEA)—limited access.

16.99 Exemption of the Immigration and Naturalization Service Systems—limited access.

16.100 Exemption of Office of Justice Programs—limited access.

16.101 Exemption of U.S. Marshals Service Systems—limited access, as indicated.

16.102 Exemption of Drug Enforcement Administration and Immigration and Naturalization Service Joint System of Records.

16.103 Exemption of the INTERPOL-United States National Central Bureau (INTERPOL USNCB) System.

16.104 Exemption of Office of Special Counsel—Waco System.

16.105 Exemption of Foreign Terrorist Tracking Task Force System.

16.106 Exemption of the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)—Access.

16.130 Exemption of Department of Justice Systems: Correspondence Management System for the Department of Justice (DOJ-003); Freedom of Information Act, Privacy Act and Mandatory Declassification Review Requests and Administrative Appeals for the Department of Justice (DOJ-004).

16.131 Exemption of Department of Justice (DOJ)/Nationwide Joint Automated Booking (JABS), DOJ-005.

16.132 Exemption of Department of Justice System—Personnel Investigation and Security Clearance Records for the Department of Justice (DOJ), DOJ-006.

16.133 Exemption of Department of Justice Regional Data Exchange System (RDEX),

DOJ-012.

Authority: 5 U.S.C. 301, 552, 552a, 552b(g), 553; 18 U.S.C. 4203(a)(1); 28 U.S.C. 509, 534; 31 U.S.C. 3717, 9701.

Subpart D—Protection of Privacy and Access to Individual Records Under the Privacy Act of 1974

Source: Order No. 2156-98, 63 FR 29600, June 1, 1998, unless otherwise noted.

§ 16.40 General provisions.

(a) *Purpose and scope.* This subpart contains the rules that the Department of Justice follows under the Privacy Act of 1974, 5 U.S.C. 552a. These rules should be read together with the Privacy Act, which provides additional information about records maintained on individuals. The rules in this subpart apply to all records in systems of records maintained by the Department that are retrieved by an individual's name or personal identifier. They describe the process by which individuals may request access to records about themselves, request amendment or correction of those records, and request an accounting of disclosures of those by the Department. In addition, the Department processes all Privacy Act requests for access to records under the Freedom of Information Act (FOIA), 5 U.S.C. 552, following the rules contained in subpart A of this part, which gives requests the benefit of both statutes.

(b) *Definitions.* As used in this subpart:

(1) *Component* means each separate bureau, office, board, division, commission, service, or administration of the Department of Justice.

(2) *Request for access* to a record means a request made under Privacy Act subsection (c)(1).

(3) *Request for amendment or correction* of a record means a request made under Privacy Act subsection (d)(2).

(4) *Request for an accounting* means a request made under Privacy Act subsection (c)(3).

(5) *Requester* means an individual who makes a request for access, a request for amendment or correction, or a request for an accounting under the Privacy Act.

(c) *Authority to request records for a law enforcement purpose.* The head of a component United States Attorney, or either's designee, is authorized to make written requests under subsection (b)(7) of the Privacy Act for records maintained by other agencies that are necessary to carry out an authorized law enforcement activity.

[Order No. 2156-98, 63 FR 29600, June 1, 1998; 63 FR 51401, Sept. 25, 1998]

§ 16.41 Requests for access to records.

(a) *How made and addressed.* You may make a request for access to a Department of Justice record about yourself by appearing in person or by writing directly to the Department component that maintains the record. Your request should be sent or delivered to the component's Privacy Act office at the address listed in appendix I to this part. In most cases, the component's central Privacy Act office is the place to send a Privacy Act request. For records held by a field office of the Federal Bureau of Investigation (FBI) or the Immigration and Naturalization Service (INS), however, you must write directly to that FBI or INS field office address, which can be found in most telephone books or by calling the component's central Privacy Act office. (The functions of each component are summarized in Part 0 of this title in the description of the Department and its components in the "United States Government Manual," which is issued annually and is available in most libraries, as well as for sale from the Government Printing Office's Superintendent of Documents. This manual also can be accessed electronically at the Government Printing Office's World Wide Web site (which can be found at http://www.access.gpo.gov/su_docs). If you cannot determine where within the Department to send your request, you may send it to the FOIA/PA Mail Referral Unit, Justice Management Division, U.S. Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001, and that office will forward it to the component(s) it believes most likely to have the records that you seek. For the quickest possible handling, you should mark both your request letter and the envelope "Privacy Act Request."

(b) *Description of records sought.* You must describe the records that you want in enough detail to enable Department personnel to locate the system of records containing them with a reasonable amount of effort. Whenever possible, your request should describe the records sought, the time periods in which you believe they were compiled, and the name or identifier number of each system of records in which you believe they are kept. The Department publishes notices in the *Federal Register* that describe its components' systems of records. A description of the Department's systems of records also may be found as part of the "Privacy

Act Compilation" published by the National Archives and Records Administration's Office of the Federal Register. This compilation is available in most large reference and university libraries. This compilation also can be accessed electronically at the Government Printing Office's Wide Web site (which can be found at http://www.access.gpo.gov/su_docs).

(c) *Agreement to pay fees.* If you make a Privacy Act request for access to records, it shall be considered an agreement by you to pay all applicable fees charged under § 16.49, up to \$25.00. The component responsible for responding to your request ordinarily shall confirm the agreement in an acknowledgement letter. When making a request, you may specify a willingness to pay a greater or lesser amount.

(d) *Verification of identity.* When you make a request for access to records about yourself, you must verify your identity. You must state your full name, current address, and date and place of birth. You must sign your request and your signature must either be notarized or subscribed to by you under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the FOIA/PA Mail Referral Unit, Justice Management Division, Department of Justice, 950 Pennsylvania Avenue, NW., Washington, DC 20530-0001. To help the identification and location of requested records, you may also, at your option, include your social security number.

(e) *Verification of guardianship.* When making a request as the parent or guardian of a minor, or as the guardian of someone determined by a court to be incompetent, for access to records about that individual, you must establish:

(1) The identity of the individual who is the subject of the record, by stating the name, current address, date and place of birth, and, at your option, the social security number of the individual;

(2) Your own identity, as required in paragraph (d) of this section;

(3) That you are the parent or guardian of that individual, which you may prove by providing a copy of the individual's birth certificate showing your parentage or by providing a court order establishing your guardianship; and

(4) That you are acting on behalf of that individual in making the request.

[Order No. 2156–98, 63 FR 29600, June 1, 1998; 63 FR 34965, June 26, 1998; 63 FR 5
Sept. 25, 1998]

§ 16.42 Responsibility for responding to requests for access to records.

(a) *In general.* Except as stated in paragraphs (c), (d), and (e) of this section, the component that first receives a request for access to a record, and has possession of that record, is the component responsible for responding to the request. In determining which records are responsive to a request, a component ordinarily shall include only those records in its possession as of the date the component begins its search for them. If any other date is specified, the component shall inform the requester of that date.

(b) *Authority to grant or deny requests.* The head of a component, or the component head's designee, is authorized to grant or deny any request for access to a record of that component.

(c) *Consultations and referrals.* When a component receives a request for access to a record not in its possession, it shall determine whether another component, or another agency of the Federal Government, is better able to determine whether the record is exempt from access under the Privacy Act. If the receiving component determines that it is best able to process the record in response to the request, then it shall do so. If the receiving component determines that it is not best able to process the record, then it shall either:

(1) Respond to the request regarding that record, after consulting with the component or agency best able to determine whether the record is exempt from access and with any other component or agency that has a substantial interest in it; or

(2) Refer the responsibility for responding to the request regarding that record to the component best able to determine whether it is exempt from access, or to another agency that originated the record (but only if that agency is subject to the Privacy Act). Ordinarily, the component or agency that originated a record will be presumed to be best able to determine whether it is exempt from access.

(d) *Law enforcement information.* Whenever a request is made for access to a record containing information that relates to an investigation of a possible violation of law and that was originated by another component or agency, the receiving component shall either refer the responsibility for responding to the request regarding that information to that other component or

or agency or shall consult with that other component or agency.

(e) *Classified information.* Whenever a request is made for access to a record containing information that has been classified by or may be appropriate for classification by another component or agency under Executive Order 12958 or any other executive order concerning the classification of records, the receiving component shall refer the responsibility for responding to the request regarding that information to the component or agency that classified the information, should consider the information for classification, or has the preponderant interest in it, as appropriate. Whenever a record contains information that has been derived from information classified by a component because it contains information classified by another component or agency, the component shall refer the responsibility for responding to the request regarding that information to the component or agency that classified the underlying information.

(f) *Notice of referral.* Whenever a component refers all or any part of the responsibility for responding to a request to another component or agency, it ordinarily shall notify the requester of the referral and inform the requester of the name of each component or agency to which the request has been referred and of the part of the request that has been referred.

(g) *Timing of responses to consultations and referrals.* All consultations and referrals shall be handled according to the date the Privacy Act access request was initially received by the component or agency, not any later date.

(h) *Agreements regarding consultations and referrals.* Components may make agreements with other components or agencies to eliminate the need for consultations or referrals for particular types of records.

[Order No. 2156–98, 63 FR 29600, June 1, 1998; 63 FR 34965, June 26, 1998; 63 FR 51000, Sept. 25, 1998]

§ 16.43 Responses to requests for access to records.

(a) *Acknowledgements of requests.* On receipt of a request, a component ordinarily shall send an acknowledgement letter to the requester which shall confirm the requester's agreement to pay fees under § 16.41(c) and provide an assigned request number for further reference.

(b) *Grants of requests for access.* Once a component makes a determination to grant a

for access in whole or in part, it shall notify the requester in writing. The component shall inform the requester in the notice of any fee charged under § 16.49 and shall disclose records to the requester promptly on payment of any applicable fee. If a request is made in person, the component may disclose records to the requester directly, in a manner not unreasonably disruptive of its operations, on payment of any applicable fee and with a written record of the grant of the request. If a requester is accompanied by another person, the requester shall be required to authorize in writing any discussion of the records in the presence of the other person.

(c) *Adverse determinations of requests for access.* A component making an adverse determination denying a request for access in any respect shall notify the requester of the determination in writing. Adverse determinations, or denials of requests, consist of: A determination to withhold any requested record in whole or in part; a determination that the requested record does not exist or cannot be located; a determination that what has been requested is not a record subject to the Privacy Act; a determination on any disputed fee matter; and a denial of a request for expedited treatment. The notification letter shall be signed by the head of the component, or the component head's designee, and shall include:

- (1) The name and title or position of the person responsible for the denial;
- (2) A brief statement of the reason(s) for the denial, including any Privacy Act exemption applied by the component in denying the request; and
- (3) A statement that the denial may be appealed under § 16.45(a) and a description of the requirements of § 16.45(a).

§ 16.44 *Classified information.*

In processing a request for access to a record containing information that is classified under Executive Order 12958 or any other executive order, the originating component shall review the information to determine whether it should remain classified. Information determined to no longer require classification shall not be withheld from a requester on the basis of Exemption (k)(1) of the Privacy Act. On receipt of any appeal involving classified information, the Office of Information and Privacy shall take appropriate action to ensure compliance with part 17 of this title.

§ 16.45 *Appeals from denials of requests for access to records.*

(a) *Appeals.* If you are dissatisfied with a component's response to your request for access to records, you may appeal an adverse determination denying your request in any respect. The Office of Information and Privacy, U.S. Department of Justice, Flag Building, Suite 570, Washington, DC 20530-0001. You must make your appeal in writing and it must be received by the Office of Information and Privacy within 60 days of the date of the letter denying your request. Your appeal letter may include as much or as little related information as you want, as long as it clearly identifies the component determination (including the assigned request number, if known) that you are appealing. For the quickest possible handling, you should enclose both your appeal letter and the envelope "Privacy Act Appeal." Unless the Attorney General directs otherwise, a Director of the Office of Information and Privacy will act on behalf of the Attorney General on all appeals under this section, except that:

(1) In the case of an adverse determination by the Deputy Attorney General or the Associate Attorney General, the Attorney General or the Attorney General's designee will act on the appeal;

(2) An adverse determination by the Attorney General will be the final action of the Department and

(3) An appeal ordinarily will not be acted on if the request becomes a matter of litigation.

(b) *Responses to appeals.* The decision on your appeal will be made in writing. A decision affirming an adverse determination in whole or in part will include a brief statement of the reason(s) for the affirmance, including any Privacy Act exemption applied, and will inform you of the Privacy Act provisions for court review of the decision. If the adverse determination is reversed or modified on appeal in whole or in part, you will be notified in a written decision and your request will be reprocessed in accordance with that appeal decision.

(c) *When appeal is required.* If you wish to seek review by a court of any adverse determination or denial of a request, you must first appeal it under this section.

§ 16.46 Requests for amendment or correction of records.

(a) *How made and addressed.* Unless the record is not subject to amendment or correction as stated in paragraph (f) of this section, you may make a request for amendment or correction of a Department of Justice record about yourself by writing directly to the Department component

that maintains the record, following the procedures in § 16.41. Your request should identify each particular record in question, state the amendment or correction that you want, and why you believe that the record is not accurate, relevant, timely, or complete. You may submit any documentation that you think would be helpful. If you believe that the same record is maintained in more than one system of records, you should state that and address your request to each component that maintains a system of records containing the record.

(b) *Component responses.* Within ten working days of receiving your request for amendment or correction of records, a component shall send you a written acknowledgment of its receipt of your request, and it shall promptly notify you whether your request is granted or denied. If a component grants your request in whole or in part, it shall describe the amendment or correction made and shall advise you of your right to obtain a copy of the corrected or amended record, in disclosable form. If the component denies your request in whole or in part, it shall send you a letter signed by the head of the component, or the component head's designee, that shall state:

(1) The reason(s) for the denial; and

(2) The procedure for appeal of the denial under paragraph (c) of this section, including the name and business address of the official who will act on your appeal.

(c) *Appeals.* You may appeal a denial of a request for amendment or correction to the Central Information and Privacy in the same manner as a denial of a request for access to records (§ 16.45) and the same procedures shall be followed. If your appeal is denied, you shall be advised of your right to file a Statement of Disagreement as described in paragraph (d) of this section and of your right under the Privacy Act for court review of the decision.

(d) *Statements of Disagreement.* If your appeal under this section is denied in whole or in part, you have the right to file a Statement of Disagreement that states your reason(s) for disagreeing with the Department's denial of your request for amendment or correction. Statements of Disagreement must be concise, must clearly identify each part of any record that is disputed, and should be no longer than one typed page for each fact disputed. Your Statement of Disagreement must be sent to the component involved, which shall place the Statement in the system of records in which the disputed record is maintained and shall mark the disputed record to indicate that a Statement of Disagreement has been filed and where in the system of records it may be found.

(e) *Notification of amendment/correction or disagreement.* Within 30 working days of the amendment or correction of a record, the component that maintains the record shall notify persons, organizations, or agencies to which it previously disclosed the record, if an account of that disclosure was made, that the record has been amended or corrected. If an individual has filed a Statement of Disagreement, the component shall append a copy of it to the disputed record whenever the record is disclosed and may also append a concise statement of its reason(s) for denying the request to amend or correct the record.

(f) *Records not subject to amendment or correction.* The following records are not subject to amendment or correction:

- (1) Transcripts of testimony given under oath or written statements made under oath;
- (2) Transcripts of grand jury proceedings, judicial proceedings, or quasi-judicial proceedings which are the official record of those proceedings;
- (3) Presentence records that originated with the courts; and
- (4) Records in systems of records that have been exempted from amendment and correction under Privacy Act, 5 U.S.C. 552a(j) or (k) by notice published in the *Federal Register*.

§ 16.47 Requests for an accounting of record disclosures.

(a) *How made and addressed.* Except where accountings of disclosures are not required to be kept (as stated in paragraph (b) of this section), you may make a request for an accounting of any disclosure that has been made by the Department to another person, organization, or agency of any record about you. This accounting contains the date, nature, and purpose of each disclosure, as well as the name and address of the person, organization, or agency to which the disclosure was made. Your request for an accounting should identify each page of the record in question and should be made by writing directly to the Department component that maintains the record, following the procedures in § 16.41.

(b) *Where accountings are not required.* Components are not required to provide an accounting of records to you where they relate to:

- (1) Disclosures for which accountings are not required to be kept—in other words, disclosures

that are made to employees within the agency and disclosures that are made under the

(2) Disclosures made to law enforcement agencies for authorized law enforcement activity in response to written requests from those law enforcement agencies specifying the law enforcement activities for which the disclosures are sought; or

(3) Disclosures made from law enforcement systems of records that have been exempted from accounting requirements.

(c) *Appeals*. You may appeal a denial of a request for an accounting to the Office of Information and Privacy in the same manner as a denial of a request for access to records under § 16.45) and the same procedures will be followed.

§ 16.48 *Preservation of records.*

Each component will preserve all correspondence pertaining to the requests that it receives under this subpart, as well as copies of all requested records, until disposition or destruction is authorized by title 44 of the United States Code or the National Archives and Records Administration's General Records Schedule 14. Records will not be disposed of while they are the subject of a pending request, appeal, or lawsuit under the Act.

§ 16.49 *Fees.*

Components shall charge fees for duplication of records under the Privacy Act in the same manner in which they charge duplication fees under § 16.11. No search or review fee may be charged for any record unless the record has been exempted from access under Exemptions (j) or (k)(2) of the Privacy Act.

§ 16.50 *Notice of court-ordered and emergency disclosures.*

(a) *Court-ordered disclosures*. When a record pertaining to an individual is required to be disclosed by a court order, the component shall make reasonable efforts to provide notice of this to the individual. Notice shall be given within a reasonable time after the component receives receipt of the order—except that in a case in which the order is not a matter of public record, the notice shall be given only after the order becomes public. This notice shall be mailed to the individual's last known address and shall contain a copy of the order and a description of the information disclosed. Notice shall not be given if disclosure is made from a criminal law

enforcement system of records that has been exempted from the notice requirement.

(b) *Emergency disclosures.* Upon disclosing a record pertaining to an individual made under compelling circumstances affecting health or safety, the component shall notify that individual of the disclosure. This notice shall be mailed to the individual's last known address and shall state the nature of the information disclosed; the person, organization, or agency to which the information was disclosed; the date of disclosure; and the compelling circumstances justifying the disclosure.

[Order No. 2156–98, 63 FR 29600, June 1, 1998; 63 FR 51401, Sept. 25, 1998]

§ 16.51 Security of systems of records.

(a) Each component shall establish administrative and physical controls to prevent unauthorized access to its systems of records, to prevent unauthorized disclosure of records, and to prevent physical damage to or destruction of records. The stringency of these controls shall correspond to the sensitivity of the records that the controls protect. At a minimum, a component's administrative and physical controls shall ensure that:

- (1) Records are protected from public view;
- (2) The area in which records are kept is supervised during business hours to prevent unauthorized persons from having access to them;
- (3) Records are inaccessible to unauthorized persons outside of business hours; and
- (4) Records are not disclosed to unauthorized persons or under unauthorized circumstances in either oral or written form.

(b) Each component shall have procedures that restrict access to records to only those individuals within the Department who must have access to those records in order to perform their duties and that prevent inadvertent disclosure of records.

[Order No. 2156–98, 63 FR 29600, June 1, 1998; 63 FR 34965, June 26, 1998]

§ 16.52 Contracts for the operation of record systems.

Any approved contract for the operation of a record system will contain the standard contract requirements issued by the General Services Administration to ensure compliance with the requirements of the Privacy Act for that record system. The contracting component will be responsible for ensuring that the contractor complies with these contract requirements.

§ 16.53 Use and collection of social security numbers.

Each component shall ensure that employees authorized to collect information are aware of:

(a) That individuals may not be denied any right, benefit, or privilege as a result of refusing to provide their social security numbers, unless the collection is authorized either by a statute or by a regulation issued prior to 1975; and

(b) That individuals requested to provide their social security numbers must be informed of:

(1) Whether providing social security numbers is mandatory or voluntary;

(2) Any statutory or regulatory authority that authorizes the collection of social security numbers; and

(3) The uses that will be made of the numbers.

§ 16.54 Employee standards of conduct.

Each component will inform its employees of the provisions of the Privacy Act, including the Act's civil liability and criminal penalty provisions. Unless otherwise permitted by law, an employee of the Department of Justice shall:

(a) Collect from individuals only the information that is relevant and necessary to discharge the responsibilities of the Department;

(b) Collect information about an individual directly from that individual whenever practicable;

(c) Inform each individual from whom information is collected of:

(1) The legal authority to collect the information and whether providing it is mandatory or

voluntary;

(2) The principal purpose for which the Department intends to use the information;

(3) The routine uses the Department may make of the information; and

(4) The effects on the individual, if any, of not providing the information;

(d) Ensure that the component maintains no system of records without public notice and notifies appropriate Department officials of the existence or development of any system records that is not the subject of a current or planned public notice;

(e) Maintain all records that are used by the Department in making any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in the determination;

(f) Except as to disclosures made to an agency or made under the FOIA, make reasonable efforts, prior to disseminating any record about an individual, to ensure that the record is accurate, relevant, timely, and complete;

(g) Maintain no record describing how an individual exercises his or her First Amendment rights, unless it is expressly authorized by statute or by the individual about whom the record is maintained, or is pertinent to and within the scope of an authorized law enforcement activity;

(h) When required by the Act, maintain an accounting in the specified form of all disclosures of records by the Department to persons, organizations, or agencies;

(i) Maintain and use records with care to prevent the unauthorized or inadvertent disclosure of a record to anyone; and

(j) Notify the appropriate Department official of any record that contains information that the Privacy Act does not permit the Department to maintain.

[Order No. 2156–98, 63 FR 29600, June 1, 1998; 63 FR 34965, June 26, 1998; 63 FR 51111, Sept. 25, 1998]

§ 16.55 Other rights and services.

Nothing in this subpart shall be construed to entitle any person, as of right, to any service or the disclosure of any record to which such person is not entitled under the Privacy Act.

Subpart E—Exemption of Records Systems Under the Privacy Act

Source: Order No. 645–76, 41 FR 12640, Mar. 26, 1976, unless otherwise noted.

§ 16.70 Exemption of the Office of the Attorney General System—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4); (d); (e) and (3), (e)(4) (G) and (H), (e)(5); and (g):

(1) General Files System of the Office of the Attorney General (JUSTICE/OAG–001).

These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), (k)(2), and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting disclosures from records concerning him/her would reveal investigative interest on the part of the Department of Justice as well as the recipient agency. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee to avoid inquiries or apprehension by law enforcement personnel.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From subsection (d) because the records contained in this system relate to official FBI investigations. Individual access to these records might compromise ongoing investigations, reveal confidential informants or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e) (1) and (5) because in the course of law enforcement investigation information may occasionally be obtained or introduced the accuracy of which is unclear which is not strictly relevant or necessary to a specific investigation. In the interests of law enforcement, it is appropriate to retain all information that may aid in establishing proof of criminal activity. Moreover, it would impede the specific investigative process if it were necessary to assure the relevance, accuracy, timeliness and completeness of all information obtained.

(5) From subsection (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation be informed of the existence of the investigation and would therefore be able to avoid detection, apprehension, or legal obligations of duties.

(6) From subsection (e)(3) because to comply with the requirements of this subsection in the course of an investigation could impede the information gathering process, thus hamper the investigation.

(7) From subsections (e)(4) (G) and (H) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(8) From subsection (g) because this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

[Order No. 31–85, 51 FR 751, Jan. 8, 1986]

§ 16.71 Exemption of the Office of the Deputy Attorney General System—limited access

(a) The following systems of records are exempt from 5 U.S.C. 552a(d)(1) and (e)(1):

(1) Presidential Appointee Candidate Records System (JUSTICE/DAG–006).

(2) Presidential Appointee Records System (JUSTICE/DAG–007).

(3) Special Candidates for Presidential Appointments Records System (JUSTICE/DAG–

(4) Miscellaneous Attorney Personnel Records System (JUSTICE/DAG-011).

These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (d)(1) because many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning a candidate for a Presidential appointment to a Department attorney position. Access could reveal the identity of the source of the information and constitute a breach of the promise of confidentiality on the part of the Department of Justice. Such breaches ultimately would restrict the free flow of information vital to a determination of a candidate's qualifications and suitability.

(2) From subsection (e)(1) because in the collection of information for investigative and evaluative purposes, it is impossible to determine in advance what exact information may be necessary for assistance in determining the qualifications and suitability of a candidate. Information which may appear irrelevant, when combined with other seemingly irrelevant information, can on occasion provide a composite picture of a candidate for a position which assists in determining whether that candidate should be nominated for appointment.

(c) The following systems of records are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(2), (3) and (5); and (g):

(1) Drug Enforcement Task Force Evaluation and Reporting System (JUSTICE/DAG-001)

(2) General Files System of the Office of the Deputy Attorney General (JUSTICE/DAG-002)

(d) In addition, the Drug Enforcement Task Force Evaluation and Reporting System is exempt from 5 U.S.C. 552a(e)(4)(G) and (H). The exemptions for the Drug Enforcement Task Force Evaluation and Reporting System apply only to the extent that information is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (K)(2). The exemptions for the General Files System apply only to the extent that information is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5).

(e) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting disclosures from records concerning him/her could reveal investigative interest on the part of the Department of Justice, as well as the recipient agency. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehension by law enforcement personnel. Further, making available to a record subject the accounting of disclosures could reveal the identity of a confidential source. In addition, release of an accounting of disclosures from the General Files System may reveal information that is properly classified pursuant to Executive Order 12356 and thereby cause damage to the national security.

(2) From subsection (c)(4) because these systems are exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From subsection (d) because the records contained in these systems relate to official Federal investigations. Individual access to these records could compromise ongoing investigations, reveal confidential informants and/or sensitive investigative techniques used in particular investigations, or constitute unwarranted invasions of the personal privacy of the parties who are involved in a certain investigation. In addition, release of records from the General Files System may reveal information that is properly classified pursuant to Executive Order 12356, and thereby cause damage to the national security. Amendment of the records in either of these systems would interfere with ongoing law enforcement proceedings and create an impossible administrative burden by requiring law enforcement investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (e)(5) because in the course of law enforcement investigations information may occasionally be obtained or introduced the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing proof of criminal activity. Moreover, it would impede any investigative process, whether civil or criminal, if it were necessary to assure the relevance, accuracy, timeliness and completeness of all information obtained.

(5) From subsection (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be informed of the existence of the investigation and may therefore be able to avoid detection.

apprehension, or legal obligations or duties.

(6) From subsection (e)(3) because to comply with the requirements of this subsection in the course of an investigation could impede the information gathering process, thus hamper the investigation.

(7) From subsections (e)(4) (G) and (H) because no access to these records is available pursuant to subsection (d) of the Privacy Act. (This exemption applies only to the Drug Enforcement Administration Force Evaluation and Reporting System.)

(8) From subsection (g) because these systems of records are exempt from the access amendment provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

[Order No. 57-91, 56 FR 58305, Nov. 19, 1991]

§ 16.72 Exemption of Office of the Associate Attorney General System—limited access

(a) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4); (d); (e)(3) and (5); and (g):

(1) General Files System of the Office of the Associate Attorney General (JUSTICE/AAG)

These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2) and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting of disclosures from records concerning him/her could reveal investigative interest on the part of the Department of Justice, as well as the recipient agency. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehension by law enforcement personnel. Further, making available to a record subject the accounting of disclosures could reveal the identity of a confidential source. In addition, release of an accounting of disclosures may reveal information that is properly classified pursuant to Executive Order 12356, and thereby cause damage to the national security.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j)(2), (k)(1), (k)(2) and (k)(5) of the Privacy Act.

(3) From subsection (d) because the records contained in this system relate to official FBI investigations. Individual access to these records could compromise ongoing investigations, reveal confidential informants and/or sensitive investigative techniques used in particular investigations, or constitute unwarranted invasions of the personal privacy of third parties involved in a certain investigation. In addition, release of these records may reveal information that is properly classified pursuant to Executive Order 12356, and thereby cause damage to the national security. Amendment of the records in this system would interfere with ongoing law enforcement proceedings and impose an impossible administrative burden requiring law enforcement investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (e)(5) because in the course of law enforcement investigations information may occasionally be obtained or introduced the accuracy of which is unclear which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing proof of criminal activity. Moreover, it would impede any investigative process, whether civil or criminal, if it were necessary to assure the relevance, accuracy, timeliness and completeness of all information obtained.

(5) From subsection (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be informed of the existence of the investigation and may therefore be able to avoid detection, apprehension, or legal obligations or duties.

(6) From subsection (e)(3) because to comply with the requirements of this subsection in the course of an investigation could impede the information gathering process, thus hamper the investigation.

(7) From subsection (g) because this system of records is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j)(2), (k)(1), (k)(2) and (k)(5) of the Privacy Act.

[Order No. 57-91, 56 FR 58305, Nov. 19, 1991]

§ 16.73 Exemption of Office of Legal Policy System—limited access.

(a) The following system of records is exempt from 5 U.S.C 552a (d)(1), (2), (3) and (4); and (2), (e)(4)(G) and (H), (e)(5); and (g):

(1) Freedom of Information and Privacy Appeals Index (JUSTICE/OLP-001).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(2) and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsections (d)(1), (2), (3), and (4) to the extent that information in this record relates to official Federal investigations and matters of law enforcement. Individual access to these records might compromise ongoing investigations, reveal confidential informants, constitute unwarranted invasions of the personal privacy of third parties who are involved in certain investigation. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(2) From subsections (e)(1) and (5) because in the course of law enforcement investigation information may occasionally be obtained or introduced the accuracy of which is unclear which is not strictly relevant or necessary to a specific investigation. In the interests of law enforcement, it is appropriate to retain all information that may aid in establishing proof of criminal activity. Moreover, it would impede the specific investigative process if it were necessary to assure the relevance, accuracy, timeliness, and completeness of all information obtained.

(3) From subsection (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation be informed of the existence of the investigation and would therefore be able to avoid detection, apprehension, or legal obligations or duties.

(4) From subsections (e)(4)(G) and (H) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(5) From subsection (g) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(c) The following system of records is exempt from 5 U.S.C. 552a(d)(1) and (e)(1):

(1) U.S. Judges Records System (JUSTICE/OLP-002).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(5).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (d)(1) because many persons are contracted who, without an assurance of anonymity, refuse to provide information concerning a candidate for a judgeship. Access to this information would reveal the identity of the source of the information and constitute a breach of the promise of confidentiality on the part of the Department. Such breaches ultimately would restrict the flow of information vital to the determination of a candidate's qualifications and suitability.

(2) From subsection (e)(1) because in the collection of information for investigative and evaluative purposes, it is impossible to determine in advance what exact information may be helpful in assisting in determining the qualifications and suitability of a candidate. Information which may seem irrelevant, when combined with other seemingly irrelevant information, can on occasion provide a composite picture of a candidate which assists in determining whether a candidate should be nominated for appointment.

(e) The following system of records is exempt from U.S.C. 552a(c) (3) and (4); (d); (e)(1) and (3), (e)(4)(G) and (H) (e)(5); and (g):

(1) General Files System of the Office of Legal Policy (JUSTICE/OLP-003).

These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5).

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting

disclosures from records concerning him/her would reveal investigative interest on the part of the Department as well as the recipient agency. This would permit record subjects to interfere with the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehension by law enforcement personnel.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From subsection (d) because the records contained in this system relate to official FBI investigations. Individual access to these records might compromise ongoing investigations, reveal confidential informants, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. Amendment of records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e) (1) and (5) because in the course of law enforcement investigations, information may occasionally be obtained or introduced the accuracy of which is unclear, which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information since it may aid in establishing patterns of criminal activity. Moreover, it would impede the specific investigation process were necessary to assure the relevance, accuracy, timeliness and completeness of all information obtained.

(5) From subsections (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be informed of the existence of the investigation and would therefore be able to avoid detection, apprehension, or legal obligations and duties.

(6) From subsection (e)(3) because to comply with the requirements of this subsection in the course of an investigation could impede the information gathering process, thus hamper the investigation.

(7) From subsections (e)(4) (G) and (H) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(8) From subsection (g) because this system is exempt from the access and amendment

provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(g) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (4); (d); (e) and (3), (e)(4)(G) and (H), (e)(5); and (g):

(1) Declassification Review System (JUSTICE/OLP-004).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552(j)(2), (k)(1), (k)(2), and (k)(5).

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting disclosures from records concerning him/her would reveal investigative interest on the part of the Department of Justice as well as the recipient agency. This would permit record subjects to impede the investigation e.g., destroy evidence, intimidate potential witnesses, or flee to avoid inquiries or apprehension by law enforcement personnel.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From subsection (d) to the extent that information in this record system relates to off duty Federal investigations and matters of law enforcement and/or is properly classified pursuant to E.O. 12356. Individual access to these records might compromise ongoing investigations, reveal confidential sources or constitute unwarranted invasions of the personal privacy of parties who are involved in a certain investigation, or jeopardize national security or foreign policy interests. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e) (1) and (5) because in the course of law enforcement investigations information may occasionally be obtained or introduced the accuracy of which is unclear or which is not strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information which may aid in establishing patterns of criminal activity. Moreover, it would impede the specific investigative process were necessary to assure the relevance, accuracy, timeliness, and completeness of all

information obtained.

(5) From subsection (e)(2) because in a law enforcement investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation be informed of the existence of the investigation and would therefore be able to avoid detection, apprehension, or legal obligations or duties.

(6) From subsection (e)(3) because to comply with the requirements of this subsection in the course of an investigation could impede the information gathering process, thus hamper the investigation.

(7) From subsections (e)(4) (G) and (H), and (g) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

[Order No. 34–85, 51 FR 754, Jan. 8, 1986. Redesignated by Order No. 6–86, 51 FR 15 Apr. 24, 1986 and further redesignated and amended by Order No. 19–86, 51 FR 39373, 28, 1986]

§ 16.74 Exemption of National Security Division Systems—limited access.

(a) The following system of records is exempted from subsections (c)(3) and (4); (d); (e)(3), (4)(G),(H) and (I), (5) and (8); (f); (g); and (h) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (2) and (5): Foreign Intelligence and Counterintelligence Records System (JUSTICE/NSD–001). These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (2), and (5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) *Subsection (c)(3).* To provide the target of a surveillance or collection activity with the disclosure accounting records concerning him or her would hinder authorized United States intelligence activities by informing that individual of the existence, nature, or scope of information that is properly classified pursuant to Executive Order 12958, as amended, and thereby cause damage to the national security.

(2) *Subsection (c)(4).* This subsection is inapplicable to the extent that an exemption is based on

claimed for subsection (d).

(3) *Subsection (d)(1)*. Disclosure of foreign intelligence and counterintelligence information would interfere with collection activities, reveal the identity of confidential sources, and cause damage to the national security of the United States. To ensure unhampered and effective collection and analysis of foreign intelligence and counterintelligence information, disclosure must be precluded.

(4) *Subsection (d)(2)*. Amendment of the records would interfere with ongoing intelligence activities thereby causing damage to the national security.

(5) *Subsections (d)(3) and (4)*. These subsections are inapplicable to the extent exemption claimed from (d)(1) and (2).

(6) *Subsection (e)(1)*. It is often impossible to determine in advance if intelligence records contained in this system are relevant and necessary, but, in the interests of national security, it is necessary to retain this information to aid in establishing patterns of activity and providing intelligence leads.

(7) *Subsection (e)(2)*. Although this office does not conduct investigations, the collection of agencies that supply information to this office would be thwarted if the agencies were required to collect information with the subject's knowledge.

(8) *Subsection (e)(3)*. To inform individuals as required by this subsection could reveal the existence of collection activity and compromise national security. For example, a target, once made aware that collection activity exists, alter his or her manner of engaging in intelligence or terrorist activities in order to avoid detection.

(9) *Subsections (e)(4)(G), (H) and (I), and (f)*. These subsections are inapplicable to the extent that this system is exempt from the access provisions of subsection (d).

(10) *Subsection (e)(5)*. It is often impossible to determine in advance if intelligence records contained in this system are accurate, relevant, timely and complete, but, in the interest of national security, it is necessary to retain this information to aid in establishing patterns of activity and providing intelligence leads.

(11) *Subsection (e)(8)*. Serving notice could give persons sufficient warning to evade

intelligence collection and anti-terrorism efforts.

(12) *Subsections (g) and (h)*. These subsections are inapplicable to the extent that this system is exempt from other specific subsections of the Privacy Act.

[Order No. 023–2007, 72 FR 44382, Aug. 8, 2007]

§ 16.75 Exemption of the Office of the Inspector General Systems/Limited Access.

(a) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e)(1), (2), (3), (5), and (8), and (g) of 5 U.S.C. 552a. In addition, the following system of records is exempted pursuant to the provision of 5 U.S.C. 552a(k)(1) and (k)(2) from subsections (c)(3), (d), and (e)(1) of 5 U.S.C. 552a:

(1) Office of the Inspector General Investigative Records (JUSTICE/OIG–001).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2). Where compliance would appear to interfere with or adversely affect the law enforcement process, and/or where it would be appropriate to permit individuals to contest the accuracy of the information collected, public source materials, the applicable exemption may be waived, either partially or totally, at the discretion of the Office of the Inspector General (OIG).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because release of disclosure accounting could alert the subjects of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and the fact that they are subjects of the investigation, and reveal investigative interest by not only the OIG, but also by the recipient agency. Since release of such information to the subjects of an investigation would provide them with significant information concerning the nature of the investigation, release could result in the destruction of documentary evidence, improper influencing of witnesses, endangerment of the physical safety of confidential sources, witnesses, and law enforcement personnel, the fabrication of testimony, flight of the subject from the area, and other activities that could impede or compromise the investigation. In addition, accounting for each disclosure could result in the release of properly classified information which would compromise the national defense and disrupt foreign policy.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of an investigation actual or potential criminal, civil, or regulatory violation, of the existence of that investigation the nature and scope of the information and evidence obtained as to his activities; of the identity of confidential sources, witnesses, and law enforcement personnel, and of information that may enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an unnecessary administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because the application of this provision could impair investigations and interfere with the law enforcement responsibilities of the OIG for the following reasons:

(i) It is not possible to detect relevance or necessity of specific information in the early stages of a civil, criminal or other law enforcement investigation, case, or matter, including investigations in which use is made of properly classified information. Relevance and necessity are questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established.

(ii) During the course of any investigation, the OIG may obtain information concerning a potential violations of laws other than those within the scope of its jurisdiction. In the interest of effective law enforcement, the OIG should retain this information, as it may aid in establishing patterns of criminal activity, and can provide valuable leads for Federal and other law enforcement agencies.

(iii) In interviewing individuals or obtaining other forms of evidence during an investigation

information may be supplied to an investigator which relates to matters incidental to the primary purpose of the investigation but which may relate also to matters under the investigative jurisdiction of another agency. Such information cannot readily be segregated.

(5) From subsection (e)(2) because, in some instances, the application of this provision presents a serious impediment to law enforcement for the following reasons:

(i) The subject of an investigation would be placed on notice as to the existence of an investigation and would therefore be able to avoid detection or apprehension, to improperly influence witnesses, to destroy evidence, or to fabricate testimony.

(ii) In certain circumstances the subject of an investigation cannot be required to provide information to investigators, and information relating to a subject's illegal acts, violations of rules of conduct, or any other misconduct must be obtained from other sources.

(iii) In any investigation it is necessary to obtain evidence from a variety of sources other than the subject of the investigation in order to verify the evidence necessary for successful litigation.

(6) From subsection (e)(3) because the application of this provision would provide the subject of an investigation with substantial information which could impede or compromise the investigation. Providing such notice to a subject of an investigation could interfere with an undercover investigation by revealing its existence, and could endanger the physical safety of confidential sources, witnesses, and investigators by revealing their identities.

(7) From subsection (e)(5) because the application of this provision would prevent the collection of any data not shown to be accurate, relevant, timely, and complete at the moment it is collected. In the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Material which may seem unrelated, irrelevant, or incomplete when collected may take on added meaning or significance as an investigation progresses. The restrictions of this provision interfere with the preparation of a complete investigative report, and thereby impede effective law enforcement.

(8) From subsection (e)(8) because the application of this provision could prematurely reveal an ongoing criminal investigation to the subject of the investigation, and could reveal

investigative techniques, procedures, or evidence.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j)(2) and (k)(1) and (k)(2) of the Privacy Act.

(c) The following system of records is exempted from 5 U.S.C. 552a(d).

(1) Office of the Inspector General, Freedom of Information/Privacy Acts (FOI/PA) Records (JUSTICE/OIG-003).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2). To the extent that information in a record pertaining to an individual does not relate to official Federal investigations and law enforcement matters, the exemption does not apply. In addition, where compliance would not appear to interfere with or adversely affect the overall law enforcement process, the applicable exemption may be waived by the Office of the Inspector General (OIG).

(d) Exemption from subsection (d) is justified for the following reasons:

(1) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of an investigation of the actual or potential criminal, civil, or regulatory violation of the existence of that investigation; the nature and scope of the information and evidence obtained as to his activities; of the identity of confidential sources, witnesses, and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an unnecessary administrative burden by requiring investigations to be continuously reinvestigated.

(2) [Reserved]

[Order No. 63–92, 57 FR 8263, Mar. 9, 1992, as amended by Order No. 64–92, 57 FR 8 Mar. 9, 1992]

§ 16.76 Exemption of Justice Management Division.

(a) The following system of records is exempt from 5 U.S.C. 552a(d):

(1) Controlled Substances Act Nonpublic Records (JUSTICE/JMD–002).

This exemption applies only to the extent that information in this system is subject to ex pursuant to 5 U.S.C. 552a(j)(2).

(b) Exemption from subsection (d) is justified for the following reasons:

(1) Access to and use of the nonpublic records maintained in this system are restricted Section 3607(b) of Title 18 U.S.C. (enacted as part of the Sentencing Reform Act of 198 L. 98–473, Chapter II) provides that the sole purpose of these records shall be for use b courts in determining whether a person found guilty of violating section 404 of the Conti Substances Act qualifies:

(i) For the disposition available under 18 U.S.C. 3607(a) to persons with no prior convict under a Federal or State law relating to controlled substances, or

(ii) For an order, under 18 U.S.C. 3607(c), expunging all official records (except the non records to be retained by the Department of Justice) of the arrest and any subsequent c proceedings relating to the offense.

(2) Information in this system consists of arrest records, including those of co-defendan records include reports of informants and investigations. Therefore, access could disclo investigative techniques, reveal the identity of confidential sources, and invade the priva third parties.

(c) The following system of records is exempted from 5 U.S.C. 552a(c)(3) and (4); (d)(1) (3), and (4); (e)(1), (2), (3), (5), and (8); and (g): Federal Bureau of Investigation Whistle

Case Files (Justice/JMD-023). These exemptions apply only to the extent that information record contained within this system is subject to exemptions pursuant to 5 U.S.C. 552a(and (k).

(d) Exemption from the particular subsections is justified for the following reasons:

(1) *Subsection (c)(3)*. To provide the subject with an accounting of disclosures of record system could inform that individual of the existence, nature, or scope of an actual or potential law enforcement or counterintelligence investigation, and thereby seriously impede law enforcement or counterintelligence efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties, civil remedies, or counterintelligence measures.

(2) *Subsection (c)(4)*. This subsection is inapplicable to the extent that an exemption is claimed for subsection (d).

(3) *Subsection (d)(1)*. Information within this record system could relate to official federal investigations and matters of law enforcement. Individual access to these records could compromise ongoing investigations, reveal confidential informants and/or sensitive investigation techniques used in particular investigations, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. Disclosure or reveal information relating to actual or potential law enforcement investigations. Disclosure of classified national security information would cause damage to the national security of the United States.

(4) *Subsection (d)(2)*. Amendment of these records could interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(5) *Subsections (d)(3) and (4)*. These subsections are inapplicable to the extent exemptions claimed from (d)(1) and (2).

(6) *Subsection (e)(1)*. It is often impossible to determine in advance if investigatory information contained in this system is accurate, relevant, timely and complete, but, in the interests of effective law enforcement and counterintelligence, it is necessary to retain this information as an aid in establishing patterns of activity and provide investigative leads.

(7) *Subsection (e)(2)*. To collect information from the subject individual could serve to notify the subject individual that he or she is the subject of a criminal investigation and thereby present a serious impediment to such investigations.

(8) *Subsection (e)(3)*. To inform individuals as required by this subsection could reveal the existence of a criminal investigation and compromise investigative efforts.

(9) *Subsection (e)(5)*. It is often impossible to determine in advance if investigatory information contained in this system is accurate, relevant, timely and complete, but, in the interests of effective law enforcement and counterintelligence, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(10) *Subsection (e)(8)*. To serve notice could give persons sufficient warning to evade investigative efforts.

(11) *Subsection (g)*. This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

[Order No. 645–76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 688–77, 42 FR 9999, Feb. 18, 1977; Order No. 899–80, 45 FR 43703, June 30, 1980; Order No. 6–86, 51 FR 15476, Apr. 24, 1986; Order No. 246–2001, 66 FR 54663, Oct. 30, 2001; Order No. 297–67 FR 70163, Nov. 21, 2002; Order No. 019–2005, 71 FR 17, Jan. 3, 2006]

§ 16.77 Exemption of U.S. Trustee Program System—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a (c) (3) and (4); (d); (e) (1) and (3), (e)(4) (G) and (H), (e) (5) and (8); (f) and (g):

(1) U.S. Trustee Program Case Referral System, JUSTICE/UST–004.

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting would permit

subject of an investigation to obtain valuable information concerning the nature of that investigation. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries or apprehensions by law enforcement personnel.

(2) From subsection (c)(4) since an exemption being claimed for subsection (d) makes that subsection inapplicable.

(3) From subsection (d) because access to the records contained in this system might compromise ongoing investigations, reveal confidential informants, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation. Amendment of the records would interfere with ongoing criminal law enforcement processes and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e)(1) and (e)(5) because in the course of law enforcement investigations information may occasionally be obtained or introduced the accuracy of which is unclear which is not strictly relevant or necessary to a specific investigation. In the interest of efficient law enforcement, it is appropriate to retain all information that may aid in establishing proof of criminal activity. Moreover, it would impede the specific investigative process if it were necessary to assure the relevance, accuracy, timeliness, and completeness of all information obtained.

(5) From subsection (e)(2) because in a criminal investigation the requirement that information be collected to the greatest extent possible from the subject individual would present an impediment to law enforcement because the subject of the investigation would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection, apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it would compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(7) From subsections (e)(4) (G) and (H) because this system of records is exempt from public access provisions of subsection (d) pursuant to subsections (j) and (k).

(8) From subsection (e)(8) because the individual notice requirement of this subsection present a serious impediment to law enforcement in that this could interfere with the U.S. Attorney's ability to issue subpoenas.

(9) From subsections (f) and (g) because this system has been exempted from the access provisions of subsection (d).

[Order No. 1-87, 52 FR 3631, Feb. 5, 1987]

§ 16.78 Exemption of the Special Counsel for Immigration-Related, Unfair Employment Practices Systems.

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (d).

(1) Central Index File and Associated Records, JUSTICE/OSC-001.

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting would permit a subject of an investigation to obtain valuable information concerning the nature of that investigation. This would permit record subjects to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid inquiries.

(2) From subsection (d) because access to the records might compromise ongoing investigations, reveal confidential informants, or constitute unwarranted invasions of the personal privacy of third parties who are involved in a certain investigation.

[Order No. 10-88, 53 FR 7735, Mar. 10, 1988]

§ 16.79 Exemption of Pardon Attorney System.

(a) The following system of records is exempt from 5 U.S.C. 552a, subsections (c)(3), (c)(d)(1), (d)(2), (d)(3), (d)(4), and (e)(5): Executive Clemency Case Files/Executive Clemency

Tracking System (JUSTICE/OPA–001). These exemptions apply only to the extent that information in this system of records is subject to exemption pursuant to 5 U.S.C. 552a(

(b) Exemption from the particular subsections is justified for the following reasons:

(1) From subsection (c)(3) because:

(i) The purpose of the creation and maintenance of the Executive Clemency Case Files/Executive Clemency Tracking System (JUSTICE/OPA–001) is to enable the Justice Department to prepare reports and recommendations to the President for his ultimate decision on clemency matters, which are committed to exclusive discretion of the President pursuant to Article II, Section 2, Clause 1 of the Constitution.

(ii) Release of the disclosure accounting, for disclosures pursuant to the routine uses published for this system, would permit the requester to obtain valuable information concerning the nature and scope of a clemency investigation, invade the right of candid and confidential communications among officials concerned with making recommendations to the President on clemency matters, and disclose the identity of persons who furnished information to the Government under an express or implied promise that their identities would be held in confidence.

(2) From subsection (c)(4) because the exemption from subsections (d)(1), (d)(2), (d)(3) and (d)(4) will make notification of disputes inapplicable.

(3) From subsections (d)(1), (d)(2), (d)(3), and (d)(4) is justified for the reasons stated in paragraph (b)(1) of this section.

(4) From subsection (e)(5) is justified for the reasons stated in paragraph (b)(1) of this section.

[Order No. 005–2003, 68 FR 4929, Jan. 31, 2003]

§ 16.80 Exemption of Office of Professional Responsibility System—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(1) and (3), (e)(4)(G) and (H), (e)(5) and (8), (f) and (g):

(1) Office of Professional Responsibility Record Index (JUSTICE/OPR-001).

These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because release of the disclosure accounting would enable the subject of an investigation to gain information concerning the existence, nature and scope of the investigation and seriously hamper law enforcement efforts.

(2) From subsections (c)(4), (d), (e)(4)(G) and (H), (f) and (g) because these provisions concern individual access to records and such access might compromise ongoing investigations, reveal confidential informants and constitute unwarranted invasions of the personal privacy of third persons who provide information in connection with a particular investigation.

(3) From subsections (e)(1) and (5) because the collection of information during an investigation necessarily involves material pertaining to other persons or events which is appropriate in a thorough investigation, even though portions thereof are not ultimately connected to the person or event subject to the final action or recommendation of the Office of Professional Responsibility.

(4) From subsection (e)(2) because collecting the information from the subject would thwart the investigation by placing the subject on notice of the investigation.

(5) From subsections (e)(3) and (e)(8) because disclosure and notice would provide the subject with substantial information which could impede or compromise the investigation. For example, an investigatory subject occupying a supervisory position could, once made aware that a misconduct investigation was ongoing, put undue pressure on subordinates so as to procure their cooperation with investigators.

(c) The following system of records is exempted from 5 U.S.C. 552a(d).

(1) Freedom of Information/Privacy Act (FOI/PA) Records (JUSTICE/OPR-002).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). To the extent that information in a record pertaining to an individual does not relate to national defense or foreign policy, official FBI investigations and/or law enforcement matters, the exemption does not apply. In addition, where compliance would not appear to interfere with or adversely affect the overall law enforcement process, the applicable exemption may be waived by OPR.

(d) Exemption from subsection (d) is justified for the following reasons:

(1) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation; the nature and scope of the information and evidence obtained as to his activities; of the identity of confidential sources, witnesses, and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information would disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an enormous administrative burden by requiring investigations to be continuously reinvestigated.

[Order No. 58–81, 46 FR 3509, Jan. 15, 1981, as amended by Order No. 159–99, 64 FR 10000, Apr. 13, 1999]

§ 16.81 Exemption of United States Attorneys Systems—limited access.

(a) The following systems of records are exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (2) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), and (g):

(1) Citizen Complaint Files (JUSTICE/USA–003).

- (2) Civil Case Files (JUSTICE/USA-005).
- (3) Consumer Complaints (JUSTICE/USA-006).
- (4) Criminal Case Files (JUSTICE/USA-007).
- (5) Kline-District of Columbia and Maryland-Stock and Land Fraud Interrelationship Filir System (JUSTICE/USA-009).
- (6) Major Crimes Division Investigative Files (JUSTICE/USA-010).
- (7) Prosecutor's Management Information System (PROMIS) (JUSTICE/USA-011).
- (8) United States Attorney, District of Columbia Superior Court Division, Criminal Files (JUSTICE/USA-013).
- (9) Pre-trial Diversion Program Files (JUSTICE/USA-014).

These exemptions apply to the extent that information in these systems is subject to exemption pursuant to U.S.C. 552a(j)(2), (k)(1) and (k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting, for disclosure pursuant to the routine uses published for these systems, would permit the subject of a criminal investigation and/or civil case or matter under investigation, litigation, regulatory administrative review or action, to obtain valuable information concerning the nature of the investigation, case or matter and present a serious impediment to law enforcement or civil activities.

(2) From subsection (c)(4) since an exemption is being claimed for subsection (d), this subsection will not be applicable.

(3) From subsection (d) because access to the records contained in these systems would inform the subject of criminal investigation and/or civil investigation, matter or case of the

existence of that investigation, provide the subject of the investigation with information that might enable him to avoid detection, apprehension or legal obligations, and present a substantial impediment to law enforcement and other civil remedies.

(4) From subsection (e)(1) because in the course of criminal investigations and/or civil investigations, cases or matters, the U.S. Attorneys often obtain information concerning violation of laws or civil obligations other than those relating to an active case or matter. In the interests of effective law enforcement and civil litigation, it is necessary that the U.S. Attorneys retain this information since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought within the U.S. Attorneys' offices.

(5) From subsection (e)(2) because in a criminal investigation the requirement that information be collected to the greatest extent possible from the subject individual would present a substantial impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection, apprehension or legal obligations and duties.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a substantial impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life and physical safety of confidential informants.

(7) From subsections (e)(4) (G) and (H) because these systems of records are exempt from individual access pursuant to subsections (j) and (k) of the Privacy Act of 1974.

(8) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(9) From subsection (e)(8) because the individual notice requirements of subsection (e)(8)

could present a serious impediment to law enforcement as this could interfere with the States Attorneys' ability to issue subpoenas and could reveal investigative techniques and procedures.

(10) From subsection (f) because these systems of records have been exempted from the access provisions of subsection (d).

(11) From subsection (g) because these systems of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

(c) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), and (g):

(1) Freedom of Information Act/Privacy Act Files (JUSTICE/USA-008)

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1) and (k)(2).

(d) Because this system contains Department of Justice civil and criminal law enforcement investigatory records, exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting would pertain to the subject of a criminal investigation and/or civil case or matter under investigation, in litigation under regulatory or administrative review or action to obtain valuable information concerning the nature of that investigation, case or matter, and present a serious impediment to law enforcement or civil legal activities.

(2) From subsection (c)(4) because an exemption is being claimed for subsection (d) of (Access to Records), rendering this subsection inapplicable to the extent that this system of records is exempted from subsection (d).

(3) From subsection (d) because access to the records contained in these systems would inform the subject of a criminal or civil investigation, matter or case of the existence of such records and provide the subject with information that might enable him to avoid detection, apprehension or legal obligations, and present a serious impediment to law enforcement.

other civil remedies. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because in the course of criminal investigations and/or civil investigations, cases or matters, the U.S. Attorneys often obtain information concerning violation of laws or civil obligations other than those relating to an active case or matter. In the interests of effective law enforcement and civil litigation, it is necessary that the U.S. Attorneys retain this information since it can aid in establishing patterns of activity and provide valuable leads for other agencies and future cases that may be brought within the U.S. Attorneys' offices.

(5) From subsection (e)(2) because to collect information to the greatest extent possible from the subject individual of a criminal investigation or prosecution would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection, apprehension, or legal obligations and duties.

(6) From subsection (e)(3) because to provide individuals supplying information with a false statement stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information, and endanger the life and physical safety of confidential informants.

(7) From subsections (e)(4) (G) and (H) because this system of records is exempt from the individual access provisions of subsection (d) and the rules provisions of subsection (f).

(8) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would inhibit the ability of trained investigator and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of intelligence necessary for effective law enforcement.

(9) From subsection (e)(8) because the individual notice requirements of subsection (e)(8)

could present a serious impediment to law enforcement as this could interfere with the Attorneys' ability to issue subpoenas and could reveal investigative techniques and procedures.

(10) From subsection (f) because this system has been exempted from the individual access provisions of subsection (d).

(11) From subsection (g) because the records in this system are generally compiled for law enforcement purposes and are exempt from the access provisions of subsections (d) and (e), rendering subsection (g) inapplicable.

(e) The following systems of records are exempt from 5 U.S.C. 552a(d)(1) and (e)(1):

(1) Assistant U.S. Attorneys Applicant Records System (JUSTICE/USA-016).

(2) Appointed Assistant U.S. Attorneys Personnel System (JUSTICE/USA-017).

These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(k)(5).

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (d)(1) because many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning a candidate for an Assistant U.S. Attorney position. Access could reveal the identity of the source of the information and constitute a breach of the promise of confidentiality on the part of the Department of Justice. Such breaches ultimately would restrict the free flow of information vital to a determination of a candidate's qualifications and suitability.

(2) From subsection (e)(1) because in the collection of information for investigative and evaluative purposes, it is impossible to determine in advance what exact information may be of assistance in determining the qualifications and suitability of a candidate. Information that may appear irrelevant, when combined with other seemingly irrelevant information, can occasionally provide a composite picture of a candidate for a position which assists in determining whether that candidate should be nominated for appointment.

(g) The *Giglio* Impeachment Files (JUSTICE/USA-018) system of records is exempt from

U.S.C. 552a subsections (c)(4), (e)(2), (e)(5), and (g) of the Privacy Act, pursuant to 5 U.S.C. 552a(j)(2), and exempt from subsections (c)(3), (d), (e)(1), (e)(4)(G) and (H), and (f), pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). These exemptions apply to the extent that information system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3); because an exemption is being claimed for subsection (d), this subsection will not be applicable.

(2) From subsection (c)(4); because an exemption is being claimed for subsection (d), this subsection will not be applicable.

(3) From subsection (d); because access to the records contained in these systems is not necessary or may impede an ongoing investigation. Most information in the records is derived from the subject's employing agency files, and individual access will be through the employing agency's files. Additionally, other information in the records may be related to allegations against an agent or witness that are currently being investigated. Providing access to this information would impede the ongoing investigation.

(4) From subsection (e)(1); because in the interest of effective law enforcement and criminal prosecution, *Giglio* records will be retained because they could later be relevant in a different case; however, this relevance cannot be determined in advance.

(5) From subsection (e)(2); because the nature of the records in this system, which are to impeach or demonstrate bias of a witness, requires that the information be collected from others.

(6) From subsections (e)(4)(G) and (H); because this system of records is exempt from individual access pursuant to subsections (j) and (k) of the Privacy Act of 1974.

(7) From subsection (e)(5); because the information in these records is not being used to make a determination about the subject of the records. According to constitutional principles of fairness articulated by the Supreme Court in *United States v. Giglio*, the records are required to be disclosed to criminal defendants to ensure fairness of criminal proceedings.

(8) From subsection (f); because records in this system have been exempted from the automatic

provisions of subsection (d).

(9) From subsection (g); because records in this system are compiled for law enforcement purposes and have been exempted from the access provisions of subsections (d) and (f).

(i) Consistent with the legislative purpose of the Privacy Act of 1974, the Executive Office of the United States Attorneys will grant access to nonexempt material in records which are maintained by the U.S. Attorneys. Disclosure will be governed by the Department's Privacy regulations, but will be limited to the extent that the identity of confidential sources will not be compromised; subjects of an investigation of an actual or potential criminal, civil or regulatory violation will not be alerted to the investigation; the physical safety of witnesses, informants, law enforcement personnel will not be endangered, the privacy of third parties will not be violated; and that the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the balance made available. The controlling principle behind this limited access is to allow disclosures except those indicated above. The decisions to release information from these systems will be made on a case-by-case basis.

[Order No. 645–76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 716–77, 42 FR 23506, May 9, 1977; Order No. 738–77, 42 FR 38177, July 27, 1977; Order No. 6–86, 51 FR 15476, Apr. 24, 1986; Order No. 57–91, 56 FR 58306, Nov. 19, 1991; Order No. 224–201, 66 FR 17809, Apr. 4, 2001]

§ 16.82 Exemption of the National Drug Intelligence Center Data Base—limited access

(a) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4); (d); (e) (1), (2), and (3); (e)(4)(I); (e) (5) and (g) of 5 U.S.C. 552a. In addition, the following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a (k)(1) and (k)(2) from subsections (c)(3), (d), and (e)(1) and (g) of 5 U.S.C. 552a:

(1) National Drug Intelligence Center Data Base (JUSTICE/NDIC–001).

(2) [Reserved]

(b) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). Where compliance would

appear to interfere with or adversely affect the law enforcement process, and/or where it would be appropriate to permit individuals to contest the accuracy of the information collected, public source materials, the applicable exemption may be waived, either partially or totally, for the National Drug Intelligence Center (NDIC). Exemptions from the particular subsection are justified for the following reasons:

- (1) From subsection (c)(3) for the same reasons that the system is exempted from the provisions of subsection (d).
- (2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsection (j)(2) of the Privacy Act.
- (3) From subsection (d) because disclosure to the subject could alert the subject of an investigation pertaining to narcotic trafficking or related activity of the fact and nature of investigation, and/or of the investigative interest of NDIC and other intelligence or law enforcement agencies (including those responsible for civil proceedings related to laws drug trafficking); lead to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; reveal the details of a sensitive investigative or intelligence technique, or the identity of a confidential source; or otherwise impede, compromise, or interfere with investigative efforts and other related law enforcement and/or intelligence activities. In addition, disclosure could invade the privacy of third parties and/or endanger the life and safety of law enforcement personnel, confidential informants, witnesses, and potential crime victims. Finally, access to records could result in the release of properly classified information that could compromise the national defense or foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations, analysis, and reports to be continuously reinvestigated and revised.
- (4) From subsection (e)(1) because, in the course of its acquisition, collation, and analysis of information, NDIC will need to retain information not immediately shown to be relevant to counterdrug law enforcement to establish patterns of activity and to assist other agencies charged with the enforcement of laws and regulations regarding drug trafficking and consistent with the acquisition of intelligence related to international aspects of drug trafficking. This consideration applies equally to information acquired from, or collated or analyzed for, law enforcement agencies and agencies of the U.S. foreign intelligence community.
- (5) From subsection (e)(2) because application of this provision could present a serious

impediment to law enforcement in that it would put the subject of an investigation, study, analysis on notice of the fact of such investigation, study, or analysis, thereby permitting subject to engage in conduct intended to frustrate the activity; because, in some circumstances, the subject of an investigation may not be required to provide to investigator certain information; and because thorough analysis and investigation may require seeking information from a number of different sources.

(6) From subsection (e)(3) (to the extent applicable) because the requirement that individuals supplying information be provided a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation and reveal the identity of confidential informants and endanger their lives and safety.

(7) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than have been published in the *Federal Register*. Should the subsection be so interpreted, exemption from this provision is necessary to protect the confidentiality of the sources of criminal and other law enforcement information and to protect the privacy and physical safety of witnesses and informants. Furthermore, greater specificity concerning the sources of properly classified records could compromise national defense or foreign policy.

(8) From subsection (e)(5) because the acquisition, collation, and analysis of information for law enforcement purposes does not permit advance determination whether such information is accurate or relevant, nor can such information be limited to that which is complete or apparently timely. Information of this type often requires further analysis and investigation to develop into a comprehensive whole that which is otherwise incomplete or even fragmented. Moreover, its accuracy is continually subject to analysis and review, and, upon careful examination, seemingly irrelevant or untimely information may acquire added significance. Additional information brings new details to light. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in collating and analyzing information and would impede the development of intelligence necessary for effective law enforcement.

(9) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement by revealing investigative techniques, procedures, or evidence.

(10) From subsection (g) to the extent that the system is exempt from subsection (d).

[Order No. 78–93, 58 FR 41038, Aug. 2, 1993]

§ 16.83 Exemption of the Executive Office for Immigration Review System—limited

(a) The following system of records is exempt from 5 U.S.C. 552a(d):

(1) The Executive Office for Immigration Review's Records and Management Information System (JUSTICE/EOIR–001).

This exemption applies only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(k) (1) and (2).

(b) Exemption from the particular subsections are justified for the following reasons:

(1) From subsection (d) because access to information which has been properly classified pursuant to an Executive Order could have an adverse effect on the national security. In addition, from subsection (d) because unauthorized access to certain investigatory materials could compromise ongoing or potential investigations; reveal the identity of confidential informants; or constitute unwarranted invasions of the personal privacy of third parties.

(2) From subsection (d) (2), (3), and (4) because the record of proceeding constitutes an official record which includes transcripts of quasi-judicial administrative proceedings, investigatory materials, evidentiary materials such as exhibits, decisional memoranda, and other case-related papers. Administrative due process could not be achieved by the ex parte "correction" of such materials by the individual who is the subject thereof.

(c) The following system of records is exempted from 5 U.S.C. 552a(d).

(1) Practitioner Compliant/Disciplinary Files (JUSTICE/EOIR 003). This exemption applies to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). To the extent that information in a record pertaining to an individual does not relate to national defense or foreign policy, official Federal investigation and/or law enforcement matters, the exemption does not apply. In addition, where compliance would not appear to interfere with or adversely affect the overall law or regulatory enforcement

process, the applicable exemption may be waived by the Executive Office for Immigration Review.

(d) Exemption from subsection (d) is justified for the following reasons:

(1) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of the investigation actual or potential criminal, civil, or regulatory violation or the existence of that investigation the nature and scope of the information and evidence obtained as to the subject's activities the identity of confidential sources, witnesses, and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. These facts would present a serious impediment to effective law and regulatory enforcement where prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel, and/or lead to the influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release properly classified information which would compromise the national defense or disrupt policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an enormous administrative burden by requiring investigations to be continuously reinvestigated.

[Order No. 18–86, 51 FR 32305, Sept. 11, 1986, as amended by Order No. 180–99, 64 FR 61787, Nov. 15, 1999]

§ 16.84 Exemption of Immigration Appeals System.

(a) The following system of records is exempt from 5 U.S.C. 552a(d) (2), (3) and (4):

(1) Decisions of the Board of Immigration Appeals (JUSTICE/BIA–001).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsections (d) (2), (3) and (4) because the decisions reflected constitute official records of opinions rendered in quasi-judicial proceedings. Administrative due process cannot be achieved by the ex parte "correction" of such opinions by the subject of the opinion.

§ 16.85 Exemption of U.S. Parole Commission—limited access.

(a) The following systems of records are exempt from 5 U.S.C. 552a (c) (3) and (4), (d), and (3), (e)(4) (G) and (H), (e)(8), (f) and (g):

(1) Docket Scheduling and Control System (JUSTICE/PRC-001).

(2) Inmate and Supervision Files System (JUSTICE/PRC-003).

(3) Labor and Pension Case, Legal File, and General Correspondence System (JUSTICE/PRC-004).

(4) Statistical, Educational and Developmental System (JUSTICE/PRC-006).

(5) Workload Record, Decision Result, and Annual Report System (JUSTICE/PRC-007)

These exemptions apply only to the extent that information in these systems is subject to exemptions pursuant to 5 U.S.C. 552a(j)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because revealing disclosure of accountings to inmates and on supervision could compromise legitimate law enforcement activities and U.S. Parole Commission responsibilities.

(2) From subsection (c)(4) because the exemption from subsection (d) will make notification disputes inapplicable.

(3) From subsection (d) because this is essential to protect internal processes by which Commission personnel are able to formulate decisions and policies with regard to federal prisoners and persons under supervision, to prevent disclosures of information to federal inmates or persons on supervision that would jeopardize legitimate correctional interests.

security, custody, supervision, or rehabilitation, to permit receipt of relevant information other federal agencies, state and local law enforcement agencies, and federal and state probation and judicial offices, to allow private citizens to express freely their opinions for or against parole, to allow relevant criminal history type information of co-defendants to be in files, to allow medical, psychiatric and sociological material to be available to professional staff and to allow a candid process of fact selection, opinion formulation, evaluation and recommendation to be continued by professional staff. The legal files contain case development material and, in addition to other reasons, should be exempt under the attorney-client privilege. Each labor or pension applicant has had served upon him the material in his file which he did not prepare and may see his own file at any time.

(4) From subsection (e)(2) because primary collection of information directly from federal inmates or persons on supervision about criminal sentence, criminal records, institutional performance, readiness for release from custody, or need to be returned to custody is highly impractical and inappropriate.

(5) From subsection (e)(3) because application of this provision to the operations and collection of information by the Commission which is primarily from sources other than the individual is inappropriate.

(6) From subsections (e)(4) (G) and (H) because exemption from the access provisions makes publication of agency procedures under (d) inapplicable.

(7) From subsection (e)(8) because the nature of the Commission's activities renders non-compliance with compulsory legal process impractical.

(8) From subsection (f) because exemption from the provisions of subsection (d) will render compliance with provisions of this subsection inapplicable.

(9) From subsection (g) because exemption from the provisions of subsection (d) will render the provisions on suits to enforce (d) inapplicable.

(c) Consistent with the legislative purpose of the Privacy Act of 1974 the U.S. Parole Commission will initiate a procedure whereby present and former prisoners and parolees obtain copies of material in files relating to them that are maintained by the U.S. Parole Commission. Disclosure of the contents will be affected by providing copies of documents

requesters through the mails. Disclosure will be made to the same extent as would be required under the substantive exemptions of the Parole Commission and Reorganization Act of 1934 (18 U.S.C. 4208) and Rule 32 of the Federal Rules of Criminal Procedure. The procedure relating to disclosure of documents may be changed generally in the interest of improving the Commission's system of disclosure or when required by pending or future decisions and directions of the Department of Justice.

[Order No. 645–76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 14–78, 43 FR 45993, Oct. 5, 1978; Order No. 899–80, 45 FR 43703, June 30, 1980; Order No. 6–86, 51 FR 15477, Apr. 24, 1986]

§ 16.88 Exemption of Antitrust Division Systems—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a (c)(3), (d), (e)(4) (G) and (f):

(1) Antitrust Caseload Evaluation System (ACES)—Monthly Report (JUSTICE/ATR–006)

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (k)(2).

(b) Exemption from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because information in this system is maintained in aid of ongoing antitrust enforcement investigations and proceedings. The release of the accounting of disclosures made under subsection (b) of the Act would permit the subject of an investigation of an actual or potential criminal or civil violation to determine whether he is the subject of the investigation. Disclosure of the accounting would therefore present a serious impediment to antitrust law enforcement efforts.

(2) From subsection (d) because access to the information retrievable from this system, if compiled for law enforcement purposes could result in the premature disclosure of the identity of the subject of an investigation of an actual or potential criminal or civil violation and information concerning the nature of that investigation. This information could enable the subject to avoid detection or apprehension. This would present a serious impediment to effective law enforcement since the subject could hinder or prevent the successful completion of the investigation. Further, confidential business and financial information, the identities

confidential sources of information, third party privacy information, and statutorily confidential information such as grand jury information must be protected from disclosure.

(3) From subsections (e)(4)(G) and (H), and (f) because this system is exempt from the individual access provisions of subsection (d).

(c) The following system of records is exempt from 5 U.S.C. 552a (c)(3), (d), (e)(4)(G) and (f):

(1) Freedom of Information/Privacy—Requester/Subject Index File (JUSTICE/ATR-008).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (k)(2).

(d) Because this system contains Department of Justice civil and criminal law enforcement investigatory records, exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the accounting of disclosures made under subsection (b) of the Act would permit the subject of an investigation of an actual or potential criminal or civil violation to determine whether he is the subject of an investigation. Disclosure of accounting would therefore present a serious impediment to antitrust law enforcement efforts.

(2) From subsection (d) because access to information in this system could result in the premature disclosure of the identity of the subject of an investigation of an actual or potential criminal or civil violation and information concerning the nature of the investigation. This information could enable the subject to avoid detection or apprehension. This would present a serious impediment to effective law enforcement since the subject could hinder or prevent successful completion of the investigation. Further, confidential business and financial information, the identities of confidential sources of information, third party privacy information, and statutorily confidential information such as grand jury information must be protected from disclosure.

(3) From subsections (e)(4)(G) and (H), and (f) because this system is exempt from the individual access provisions of subsection (d).

[Order No. 2–86, 51 FR 884, Jan. 9, 1986]

§ 16.89 Exemption of Civil Division Systems—limited access.

(a) The following systems of records are exempted pursuant to 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e)(1), (e)(2), (e)(3), (e)(4) (G) and (H), (e)(5), (e)(8), and in addition, the following systems of records are exempted pursuant to 5 U.S.C. 552a (k)(1) and (k)(2) from subsections (c)(3), (d), (e)(1), (e)(4) (G) and (H):

(1) Civil Division Case File System, JUSTICE/CIV–001.

(2) Freedom of Information/Privacy Acts File System, JUSTICE/CIV–005.

These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2).

(b) Only that information which relates to the investigation, prosecution, or defense of a potential criminal or civil litigation, or which has been properly classified in the interest of national defense and foreign policy is exempted for the reasons set forth from the following subsections:

(1) *Subsection (c)(3)*. To provide the subject of a criminal or civil matter or case under investigation with an accounting of disclosures of records concerning him or her would identify that individual (and others to whom the subject might disclose the records) of the existence, nature, or scope of that investigation and thereby seriously impede law enforcement efforts in permitting the record subject and others to avoid criminal penalties and civil remedies.

(2) *Subsections (c)(4), (e)(4) (G) and (H), and (g)*. These provisions are inapplicable to the extent that these systems of records are exempted from subsection (d).

(3) *Subsection (d)*. To the extent that information contained in these systems has been properly classified, relates to the investigation and/or prosecution of grand jury, civil fraud, and other law enforcement matters, disclosure could compromise matters which should be kept secret in the interest of national security or foreign policy; compromise confidential investigations and proceedings; hamper sensitive civil or criminal investigations; impede affirmative enforcement actions based upon alleged violations of regulations or of civil or criminal laws; reveal the

identity of confidential sources; and result in unwarranted invasions of the privacy of others. Amendment of the records would interfere with ongoing criminal law enforcement processes and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) *Subsection (e)(1)*. In the course of criminal or civil investigations, cases, or matters, the Division may obtain information concerning the actual or potential violation of laws which is not strictly within its statutory authority. In the interest of effective law enforcement, it is necessary to retain such information since it may establish patterns of criminal activity or avoidance of other civil obligations and provide leads for Federal and other law enforcement agencies.

(5) *Subsection (e)(2)*. To collect information from the subject of a criminal investigation or prosecution would present a serious impediment to law enforcement in that the subject or others to whom the subject might be in contact) would be informed of the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6) *Subsection (e)(3)*. To comply with this requirement during the course of a criminal investigation or prosecution could jeopardize the investigation by disclosing the existence of a confidential investigation, revealing the identity of witnesses or confidential informants, or impeding the information gathering process.

(7) *Subsection (e)(5)*. In compiling information for criminal law enforcement purposes, the accuracy, completeness, timeliness and relevancy of the information obtained cannot always be immediately determined. As new details of an investigation come to light, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can often only be determined in a court of law. Compliance with this requirement would therefore restrict the ability of government attorneys in exercising their judgment in developing information necessary for effective law enforcement.

(8) *Subsection (e)(8)*. To serve notice would give persons sufficient warning to evade law enforcement efforts.

(c) The following system of records is exempted pursuant to 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e)(1) and (e)(5); in addition, this system is also exempted

pursuant to 5 U.S.C. 552a(k)(2) from subsections (c)(3), (d), and (e)(1).

Consumer Inquiry/Investigatory System, JUSTICE/CIV-006.

These exemptions apply only to the extent that information in this system of records is s
to exemption pursuant to 5 U.S.C. 552a (j)(2) and (k)(2).

(d) Only that information compiled for criminal or civil law enforcement purposes is exen
for the reasons set forth from the following subsections:

(1) *Subsections (c)(3)*. This system occasionally contains investigatory material based o
complaints of actual or alleged criminal or civil violations. To provide the subject of a cri
civil matter or case under investigation with an accounting of disclosures of records con
him/her would inform that individual of the existence, nature, or scope of that investigati
thereby seriously impede law enforcement efforts by permitting the record subject and c
persons to whom he might disclose the records to avoid criminal penalties and civil rem

(2) *Subsections (c)(4)*. This subsection is inapplicable to the extent that an exemption is
claimed for subsection (d).

(3) *Subsection (d)*. Disclosure of information relating to the investigation of complaints o
alleged violation of criminal or civil law could interfere with the investigation, reveal the ic
of confidential sources, and result in an unwarranted invasion of the privacy of others.
Amendment of the records would interfere with ongoing criminal law enforcement proce
and impose an impossible administrative burden by requiring criminal investigations to b
continuously reinvestigated.

(4) *Subsection (e)(1)*. In the course of criminal or civil investigations, cases, or matters, t
Division may obtain information concerning the actual or potential violation of laws which
not strictly within its statutory authority. In the interest of effective law enforcement, it is
necessary to retain such information since it may establish patterns of criminal activity o
avoidance of other civil obligations and provide leads for Federal and other law enforcer
agencies.

(5) *Subsection (e)(5)*. In compiling information for criminal law enforcement purposes, th
accuracy, completeness, timeliness and relevancy of the information obtained cannot al

be immediately determined. As new details of an investigation come to light, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can often only be determined in a court of law. Compliance with this requirement would therefore restrict the ability of government attorneys in exercising their judgment developing information necessary for effective law enforcement.

(e) The following system of records is exempt pursuant to 5 U.S.C. 552a (j)(2) and (k)(2) subsection (d):

Congressional and Citizen Correspondence File, JUSTICE/CIV-007.

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C 552a (j)(2) and (k)(2).

(f) Only that portion of the Congressional and Citizen Correspondence File maintained in the Communications Office which consists of criminal or civil investigatory information is exempt for the reasons set forth from the following subsection:

(1) *Subsection (d)*. Disclosure of investigatory information would jeopardize the integrity of the investigative process, disclose the identity of individuals who furnished information to the government under an express or implied promise that their identities would be held in confidence, and result in an unwarranted invasion of the privacy of others. Amendment records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

[Order No. 27-88, 54 FR 113, Jan. 4, 1989]

§ 16.90 Exemption of Civil Rights Division Systems.

(a) The following system of records is exempted from subsections (c)(3) and (4); (d)(1), (2), and (4); (e)(1), (2), (3), (5), and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k): Central Civil Rights Division Index File and Associated Records (JUSTICE/CRT-001). These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) *Subsection (c)(3)*. To provide the subject of a criminal, civil, or administrative matter under investigation with an accounting of disclosures of records concerning him or her or to inform that individual of the existence, nature, or scope of an actual or potential criminal violation to gain valuable information concerning the nature and scope of the investigation to determine whether he or she is the subject of the investigation, and seriously impede law enforcement efforts by permitting the record subject and other persons to whom he or she might disclose the records to avoid criminal penalties, civil remedies, or administrative measures.

(2) *Subsection (c)(4)*. This subsection is inapplicable to the extent that an exemption is claimed for subsection (d).

(3) *Subsection (d)(1)*. Disclosure of investigatory information could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others. Disclosure of classified national security information would cause damage to the national security of the United States. In addition, these records may be subject to protective orders entered by federal courts to protect their confidentiality. Further, many of the records contained in this system are copies of documents which are the property of agencies and were obtained under express or implied promises to strictly protect their confidentiality.

(4) *Subsection (d)(2)*. Amendment of the records could interfere with ongoing criminal or law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(5) *Subsection (d)(3) and (4)*. These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) *Subsection (e)(1)*. It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interest of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(7) *Subsection (e)(2)*. To collect information from the subject individual could serve notice

he or she is the subject of a criminal investigation and thereby present a serious impediment to such investigation.

(8) *Subsection (e)(3)*. To inform individuals as required by this subsection could reveal the existence of a criminal or civil investigation and compromise investigative efforts.

(9) *Subsection (e)(5)*. It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interest of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(10) *Subsection (e)(8)*. To serve notice could give persons sufficient warning to evade investigative efforts.

(11) *Subsection (g)*. This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

(c) The following system of records is exempted from subsections (d)(1), (2), (3) and (4) of the Privacy Act pursuant to 5 U.S.C. 552a (k): "Files on Employment Civil Rights Matters Referred by the Equal Employment Opportunity Commission (JUSTICE/CRT-007)." These exemptions apply only to the extent that information in a record is subject to exemption pursuant to U.S.C. 552a (k)(2).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) *Subsection (d)(1)*. Disclosure of investigatory information could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others. In addition, these records may be subject to protective orders issued by federal courts to protect their confidentiality. Further, many of the records contained in the system are copies of documents which are the property of state agencies and were obtained under express or implied promises to strictly protect their confidentiality.

(2) *Subsection (d)(2)*. Amendment of the records could interfere with ongoing criminal or civil law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(3) *Subsection (d)(1), (2), (3) and (4)*. This system contains investigatory material compiled

the Equal Opportunity Commission pursuant to its authority under 42 U.S.C. 2000e–8. 7 U.S.C. 2000e–5(b), 42 U.S.C. 2000e–8(e), and 44 U.S.C. 3508 make it unlawful to make in any manner whatsoever any information obtained by the Commission pursuant to the authority.

(4) *Subsection (d)(3) and (4).* These subsections are inapplicable to the extent exemption claimed from (d)(1) and (2).

[Order No. 019–2003, 68 FR 61622, Oct. 29, 2003]

§ 16.91 Exemption of Criminal Division Systems—limited access, as indicated.

(a) The following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (1), (2) and (3), (e)(4) (G), (H) and (I) and (8), (f) and (g) of 5 U.S.C. 552a; in addition, the following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a (k)(1) and (k)(2) from subsections (c)(3), (d) (e)(4) (G), (H), and (I), and (f) of 5 U.S.C. 552a:

(1) Central Criminal Division, Index File and Associated Records System of Records (JUSTICE/CRM–001)—Limited Access. This system of records and associated exemption adopted by and applies with equal force and effect to the National Security Division, unmodified, superseded, or revoked in accordance with law.

(2) General Crimes Section, Criminal Division, Central Index File and Associated Records System of Records (JUSTICE/CRM–004)—Limited Access.

These exemptions apply to the extent that information in those systems are subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2).

(b) The systems of records listed under paragraphs (b)(1) and (b)(2) of this section are exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(3). The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for systems of records, would permit the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to determine whether he is the subject of investigat

to obtain valuable information concerning the nature of that investigation, and the information obtained, or the identity of witnesses and informants and would therefore present a serious impediment to law enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this subsection is inapplicable to the extent that these systems of records are exempted from subsection (d).

(3). (d). Access to the records contained in these systems would inform the subject of a investigation of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation, or the nature and scope of the information and evidence obtained as a result of activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, could lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4). (e)(1). The notices of these systems of records published in the *Federal Register* set forth the basic statutory or related authority for maintenance of this system. However, in the course of criminal or other law enforcement investigations, cases, and matters, the Criminal Division and its components will occasionally obtain information concerning actual or potential violations of law that are not strictly within its statutory or other authority or may compile information in the course of an investigation which may not be relevant to a specific prosecution. In the interest of effective law enforcement, it is necessary to retain such information in these systems of records since it can aid in establishing patterns of criminal activity and can provide valuable leads for federal and other law enforcement agencies.

(5). (e)(2). In a criminal investigation or prosecution, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6). (e)(3). The requirement that individuals supplying information be provided with a for stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or the identity of witnesses or confidential informants.

(7). (e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency) and (d) (Access to Records) of the Act these subsections are inapplicable to the extent these systems of records are exempted from subsections (f) and (d).

(8). (e)(4)(I). The categories of sources of the records in these systems have been published in the *Federal Register* in broad generic terms in the belief that this is all that subsection (I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal and law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(9). (e)(5). In the collection of information for criminal law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance. Further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators, intelligence analysts, and government attorneys in exercising their judgment in reporting on information and investigations and impede the development of criminal or other intelligence necessary for effective law enforcement.

(10). (e)(8). The individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.

(11). (f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an actual or potential criminal, civil, or regulatory investigation or prosecution must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation or prosecution pending or future. In addition, mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of an investigation.

and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the requirements pursuant to subsection (f) (2) through (5) are inapplicable to these systems of records to the extent that these systems of records are exempted from subsection (d).

(12). (g). Since an exemption is being claimed for subsections (d) (Access to Records) and (e) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for subsections (d) and (e), to the extent that these systems of records are exempted from subsections (d) and (e).

(13). In addition, exemption is claimed for these systems of records from compliance with the following provisions of the Privacy Act of 1974 (5 U.S.C. 552a) pursuant to the provision U.S.C. 552a(k)(1): Subsections (c)(3), (d), (e)(1), (e)(4) (G), (H) and (I) and (f) to the extent that the records contained in these systems are specifically authorized to be kept secret in the interests of national defense and foreign policy.

(c) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a (2) from subsection (c) (3) and (4), (d), (e) (1), (2) and (3), (e) (4) (G), (H) and (I), (e) (5) (8), (f) and (g) of 5 U.S.C. 552a:

Criminal Division Witness Security File System of Records (JUSTICE/CRM-002).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(d) The system of records listed under paragraph (c) of this section is exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(3) The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would permit the subject of an investigation of an actual or potential criminal violation, which may include those protected under the Witness Security Program, to determine whether he is the subject of a criminal investigation, to obtain valuable information concerning the nature of that investigation and the information obtained, or the identity of

witnesses and informants and the nature of their reports, and would therefore present a serious impediment to law enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement subsection (f)(1) is specifically exempted for these systems of records. Moreover, disclosure of the accounting to an individual protected under the Witness Security Program could jeopardize the effectiveness and security of the Program by revealing the methods and techniques utilized in relocating witnesses and could therefore jeopardize the ability to conduct and to protect the confidentiality of, information compiled for purposes of a criminal investigation.

(2). (c)(4) Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable.

(3). (d) Access to the records contained in these systems would inform the subject of an investigation of an actual or potential criminal violation, which may include those protected under the Witness Security Program, of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and lead to the improper influence of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, access to the records in these systems to an individual protected under the Witness Security Program could jeopardize the effectiveness and security of the Program by revealing the methods and techniques utilized in relocating witnesses and could therefore jeopardize the ability to conduct and to protect the confidentiality of, information compiled for purposes of a criminal investigation.

(4). Exemption is claimed from subsection (e)(1) for the reasons stated in subsection (b) of this section.

(5). (e)(2) In the course of preparing a Witness Security Program for an individual, much information is collected from the subject. However, the requirement that the information be collected to the greatest extent practicable from the subject individual would present a serious impediment to criminal law enforcement because the individual himself may be the subject of a criminal investigation or have been a participant in, or observer of, criminal activity. As a result, it is necessary to seek information from other sources. In addition, the failure to verify the

information provided from the individual when necessary and to seek other information ()
jeopardize the confidentiality of the Witness Security Program and lead to the obtaining
maintenance of incorrect and uninvestigated information on criminal matters.

(6). (e)(3) The requirement that individuals supplying information be provided with a form
stating the requirements of subsection (e)(3) would constitute a serious impediment to law
enforcement in that it could compromise or reveal the identity of witnesses and informants
protected under the Witness Security Program.

(7). (e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency
and (d) (Access to Records) of the Act these subsections are inapplicable.

(8). (e)(4)(I). The categories of sources of the records in these systems have been published
in the *Federal Register* in broad generic terms in the belief that this is all that subsection (I)
of the Act requires. In the event, however, that this subsection should be interpreted to
more detail as to the identity of sources of the records in the system, exemption from the
provision is necessary in order to protect the confidentiality of the sources of criminal law
enforcement information and of witnesses and informants protected under the Witness
Security Program.

(9). Exemption is claimed from subsections (e)(5) and (e)(8) for the reasons stated in
subsection (b)(9) and (b)(10) of this section.

(10). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence
of records contained in these systems pertaining to him would inform the subject of an
investigation of an actual or potential criminal violation, which may include those protected
under the Witness Security Program, of the existence of that investigation, of the nature
and scope of the information and evidence obtained as to his activities, of the identity of witnesses
and informants, or would provide information that could enable the subject to avoid detection
or apprehension. These factors would present a serious impediment to effective law
enforcement because they could prevent the successful conduct and/or completion of an
investigation pending or future, endanger the physical safety of witnesses or informants
lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication
of testimony. In addition, notices as to the existence of records contained in these systems
to an individual protected under the Witness Security Program could jeopardize the effectiveness
and security of the Program by revealing the methods and techniques utilized in relocating
witnesses and could therefore jeopardize the ability to obtain, and to protect the confidence

of, information compiled for purposes of a criminal investigation.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the requirements pursuant to subsection (f) (2) through (5) are inapplicable.

(11). (g) Since an exemption is being claimed for subsections (d) (Access to Records) and (e) (Agency Rules) this section is inapplicable and is exempted for the reasons set forth for subsections.

(e) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (4) (G), (H) and (I), (f), and (g) of 5 U.S.C. 552a:

Organized Crime and Racketeering Section, Intelligence and Special Services Unit, Info Request System of Records (JUSTICE/CRM-014).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(f) The system of records listed under paragraph (e) of this section is exempted for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(3). The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would permit the subject of an investigation of an actual or potential criminal violation to determine whether he is the subject of a criminal investigation and would therefore present a serious impediment to law enforcement. The records in these systems contain the names of the subjects of the files in question and the system is accessible by the name of the person checking out the file and by name of the subject of the file. In addition, the disclosure of the accounting would amount to notice to the individual of the existence of the record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable.

(3). (d). Access to the records contained in these systems would inform the subject of a

investigation of an actual or potential criminal violation of the existence of that investigation. This would present a serious impediment to effective law enforcement because it could the successful completion of the investigation, endanger the physical safety of witnesses, informants, and lead to the improper influencing of witnesses, the destruction of evidence, the fabrication of testimony.

(4). Exemption is claimed from subsections (e)(4) (G), (H) and (I) for the reasons stated subsections (b)(7) and (b)(8) of this section.

(5). (f). These systems may be accessed by the name of the person who is the subject of the file and who may also be the subject of a criminal investigation. Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him, may deal with an actual or potential criminal investigation or prosecution, must be exempt because such notice to an individual would be detrimental to the successful conduct and completion of the investigation or prosecution pending or future. In addition mere notice of the fact of an investigation could inform the subject or others that their activities are under scrutiny and become the subject of an investigation and could enable the subjects to avoid detection and apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the exemptions required pursuant to subsection (f) (2) through (5) are inapplicable.

(6). (g). Since an exemption is being claimed for subsections (d) (Access to Records) and (e) (Agency Rules) of the Act this section is inapplicable and is exempted for the reasons stated for those subsections.

(g) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c)(4), (d), (e)(4) (G), (H) and (I), (f) and (g) of 5 U.S.C. 552a.

File of Names Checked to Determine If Those Individuals Have Been the Subject of an Electronic Surveillance System of Records (JUSTICE/CRM-003).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(h) The system of records listed under paragraph (g) of this section is exempted, for the

reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable to the extent that this system of records is exempted under subsection (d).

(2). (d). The records contained in this system of records generally consist of information filed with the court in response to the request and made available to the requestor. To the extent that these records have been so filed, no exemption is sought from the provisions of this subsection. Occasionally, the records contain pertinent logs of intercepted communications and other investigative reports not filed with the court. These records must be exempted because access to such records could inform the subject of an investigation of an actual or potential criminal violation of the existence of that investigation and of the nature of the information and evidence obtained by the government. This would present a serious impediment to effective law enforcement because it could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(3). Exemption is claimed from subsections (e)(4) (G), (H) and (I) for the reasons stated under subsections (b)(7) and (b)(8) of this section.

(4). (f). The records contained in this system of records generally consist of information filed with the court and made available to the requestor. To the extent that these records have been so filed, no exemption is sought from the provisions of this subsection. Occasionally, the records contain pertinent logs of intercepted communications and other investigative reports not filed with the court. These records must be exempted from a requirement of notification of their existence because such notice to an individual would be detrimental to the successful conduct and/or completion of a criminal investigation or prosecution pending or future. In addition, mere notice of the existence of such logs or investigative reports could inform the subject or others that their activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the provisions required pursuant to subsection (f) (2) through (5) are inapplicable to the extent that this system of records is exempted for subsection (d).

(6). (g). Since an exemption is being claimed for subsections (d) (Access to Records) and (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for subsections, to the extent that this system of records is exempted from subsections (d)

(i) The following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (1), (2), and (3), (e)(4) (G), (H), and (5) and (8), (f) and (g) of 5 U.S.C. 552a:

(1) Information File on Individuals and Commercial Entities Known or Suspected of Being Involved in Fraudulent Activities System of Records (JUSTICE/CRM-006).

(2) The Stocks and Bonds Intelligence Control Card File System of Records (JUSTICE/CRM-021).

(3) Tax Disclosure Index File and Associated Records (JUSTICE/CRM-025).

These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(j) The systems of records listed in paragraphs (i)(1), (i)(2), and (i)(3) of this section are exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1)(c)(3) The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the act, including those permitted under the routine uses published for these systems of records, would permit the subject of an investigation of an actual or potential criminal violation to determine whether he is the subject of a criminal investigation, to obtain valuable information concerning the nature of that investigation, and the information obtained, or the identity of witnesses and informants, and would therefore present a serious impediment to law enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for this system of records.

(2)(c)(4) Since an exemption is being claimed for subsection (d) of the act (access to records) this section is inapplicable to the extent that these systems of records are exempted from subsection (d).

(3)(d) Access to the records contained in these systems would inform the subject of an investigation of an actual or potential criminal violation of the existence of that investigation, the nature and scope of the information and evidence obtained as to his activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, and lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4) Exemption is claimed from subsections (e) (1), (2), and (3), (e)(4) (G), (H), and (I), (e)(5), (e)(6), (e)(7), (e)(8), (e)(9), and (e)(10) for the reasons stated in subsections (b)(4), (b)(5), (b)(6), (b)(7), (b)(8), (b)(9), and (b)(10) of this section.

(5)(f) Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an actual or potential criminal investigation or prosecution must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation or prosecution pending or in progress. In addition, mere notice of the fact of an investigation could inform the subject or others of their activities are under or may become the subject of an investigation and could enable subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony. Since an exemption is being claimed for subsection (d) (access to records), the rules required pursuant to subsection (f) (2) through (5) are inapplicable to these systems of records.

(6)(g) Since an exemption is being claimed for subsections (d) (access to records) and (e) (Agency rules), this section is inapplicable and is exempted for the reasons set forth for subsections.

(k) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (1), (2) and (3), (e)(4) (G), (H) and (I) and (8), (f) and (g) of 5 U.S.C. 552a; in addition, the following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a(k)(1) from subsections (c) (3), (d), (e)(1), (e)(2), (e)(4) (G), (H) and (I) and (f) of 5 U.S.C. 552a:

Organized Crime and Racketeering Section, Criminal Division, General Index File and Associated Records System of Records (JUSTICE/CRM-012).

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(1).

(l) The system of records listed under paragraph (m) ¹ of this section is exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

¹ Paragraph (m) was redesignated as paragraph (k) at 44 FR 54046, Sept. 18, 1979.

(1). Exemption is claimed from subsections (c) (3) and (4) and (d) for the reasons stated in subsections (j)(1), (j)(2) and (j)(3) of this section.

(2). (e)(1). The notice for this system of records published in the *Federal Register* sets forth the basic statutory or related authority for maintenance of this system. However, in the course of criminal investigations, cases, and matters, the Organized Crime and Racketeering Section occasionally obtain information concerning actual or potential violations of law that are not strictly within its statutory or other authority, or may compile information in the course of investigation which may not be relevant to a specific prosecution. In the interests of effective law enforcement, it is necessary to retain such information in this system of records since it aids in establishing patterns of criminal activity and can provide valuable leads for federal and other law enforcement agencies.

(3). Exemption is claimed from subsections (e) (2) and (3), (e)(4) (G), (H) and (I), (e) (5) (8), (f) and (g) for the reasons stated in subsections (b)(5), (b)(6), (b)(7), (b)(8), (b)(9), (b)(10), (b)(11) and (b)(12) of this section.

(4). In addition, exemption is claimed for this system of records from compliance with the following provisions of the Privacy Act of 1974 (5 U.S.C. 552a) pursuant to the provision 5 U.S.C. 552a(k)(1): Subsections (c)(3), (d), (e)(1), (e)(4) (G), (H) and (I) and (f) to the extent that the records contained in this system are specifically authorized to be kept secret in the interests of national defense and foreign policy.

(m) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (2) and (3), (e) (4) (G), (H) and (I), (e) (5) (8), (f) and (g) of 5 U.S.C. 552a:

Requests to the Attorney General For Approval of Applications to Federal Judges For

Electronic Interceptions System of Records (JUSTICE/CRM-019).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(n) The system of records listed in paragraph (m) of this section is exempted for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

(1). (c)(3). The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would permit the subject of an electronic interception to obtain valuable information concerning the interception, including information as to whether he is the subject of a criminal investigation, by means other than those provided for by statute. Such information could interfere with the successful conduct and/or completion of a criminal investigation and therefore present a serious impediment to law enforcement. In addition, disclosure accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable.

(3). (d). Access to the records contained in these systems would inform the subject of a criminal investigation of the existence of such surveillance including information as to whether he is the subject of a criminal investigation by means other than those provided for by statute. This could interfere with the successful conduct and/or completion of a criminal investigation and therefore present a serious impediment to law enforcement.

(4). (e)(2). In the context of an electronic interception, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and this would therefore decrease the efficacy of the interception.

(5). (e)(3). The requirement that individuals supplying information be provided with a statement stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential electronic interception.

or reveal the identity of witnesses or confidential informants.

(6). (e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency and (d) (Access to Records) of the Act these subsections are inapplicable.

(7). Exemption is claimed from subsections (e)(4)(I) and (e)(8) for the reasons stated in subsections (b)(8) and (b)(10) of this section.

(8). (f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an electronic interception other than pursuant to statute must be exempted because such notice to an individual would be detrimental to successful conduct and/or completion of an investigation pending or future. In addition, notice of the fact of an electronic interception could inform the subject or others that the activities are under or may become the subject of an investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the required pursuant to subsection (f)(2) through (5) are inapplicable to these systems of records to the extent that these systems of records are exempted from subsection (d).

(9). (g). Since an exemption is being claimed for subsection (d) (Access to Records) and (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for subsections, to the extent that these systems of records are exempted from subsection (f).

(o) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (4), (d), (e) (2) and (3), (e) (4) (G), (H), and (I), (f) and (g) of 5 U.S.C. 552a; in addition the following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(k)(1) and (k)(2) from subsections (c)(3), (d), (e)(4) (G), (H), (I), and (f) of 5 U.S.C. 552a:

Witness Immunity Records System of Records (JUSTICE/CRM-022).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and (k)(1) and (k)(2).

(p) The system of records listed under paragraph (q) ² of this section is exempted, for the reasons set forth, from the following provisions of 5 U.S.C. 552a:

² Paragraph (q) was redesignated as paragraph (o) at 44 FR 54046, Sept. 18, 1979.

(1). (c)(3). Release of the accounting of disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for this system of records as to a witness for whom immunity has been proposed, would inform the individual of the existence of the proposed immunity prematurely, thus creating a serious impediment to effective law enforcement in that the witness could flee, destroy evidence, or fabricate testimony; and (b) as to a witness to whom immunity has been granted, or for whom it has been denied, would reveal the nature and scope of the activities, if any, of the witness known to the government, which would also create a serious impediment to effective law enforcement.

(2). (c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records) this section is inapplicable to the extent that this system of records is exempted from subsection (d).

(3). (d). Access to the records contained in this system (a) as to a witness for whom immunity has been proposed, would inform the individual of the existence of the proposed immunity prematurely, thus presenting a serious impediment to effective law enforcement in that the witness could flee, destroy evidence, or fabricate testimony; and (b) as to a witness to whom immunity has been granted, or for whom it has been denied, would reveal the nature and scope of the activities, if any, of the witness known to the government, which would also create a serious impediment to effective law enforcement.

(4). (e)(2). In a witness immunity request matter, the requirement that information be disclosed to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the immunity request and often the subject of the underlying investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(5). Exemption is claimed from subsections (e)(3), (e)(4)(G), (H) and (I), and (e)(8) for the reasons stated in subsections (b)(6), (b)(7), (b)(8) and (b)(10) of this section.

(6). (f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him (a) as to a witness for whom immunity has been proposed, inform the individual of the existence of the proposed immunity prematurely, thus present a serious impediment to effective law enforcement in that the witness could flee, destroy evidence, or fabricate testimony; and (b) as to a witness to whom immunity has been granted or for whom it has been denied, would reveal the nature and scope of the activity, if any witness known to the government, which would also create a serious impediment to effective law enforcement.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the exemptions required pursuant to subsection (f)(2) through (5) are inapplicable to this system of records to the extent that this system of records is exempted from subsection (d).

(7). (g). Since an exemption is being claimed for subsections (d) (Access to Records) and (e) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for subsections (d) and (e), to the extent that this system of records is exempted for subsections (d) and (e).

(8). In addition, exemption is claimed for this system of records from compliance with the following provisions of the Privacy Act of 1974 (5 U.S.C. 552a) pursuant to the provision 5 U.S.C. 552a(k)(1): subsections (c)(3), (d), (e)(1), (e)(4) (G), (H) and (I) and (f) to the extent that the records contained in this system are specifically authorized to be kept secret in the interests of national defense and foreign policy.

(q) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) and (3), (e)(4) (G), (H) and (I), (e) (5) and (8), (f), and (g):

(1) Freedom of Information/Privacy Act Records (JUSTICE/CRM-024)

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1) and (k)(2).

(r) Because this system contains Department of Justice civil and criminal law enforcement investigatory records, it is exempted for the reasons set forth from the following provision of 5 U.S.C. 552a:

(1)(c)(3). The release of the disclosure accounting would present a serious impediment

enforcement by permitting the subject of an investigation of an actual or potential criminal or regulatory violation to determine whether he is the subject of investigation, or to obtain valuable information concerning the nature of that investigation and the information obtained or to identify witnesses and informants.

(2)(c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records), this subsection is inapplicable to the extent that this system of records is exempt from subsection (d).

(3)(d). Access to records contained in this system would enable the subject of an investigation of an actual or potential criminal or civil case or regulatory violation to determine whether she is the subject of investigation, to obtain valuable information concerning the nature and scope of the investigation, and information or evidence obtained as to his/her activities, to identify witnesses and informants, or to avoid detection or apprehension. Such results could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony, and thereby present a serious impediment to criminal law enforcement. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4)(e)(1). In the course of criminal or other law enforcement investigations, cases, and matters, the Criminal Division will occasionally obtain information concerning actual or potential violations of law that are not strictly within its statutory or other authority, or it may compile information in the course of an investigation which may not be relevant to a specific prosecution. In the interests of effective law enforcement, it is necessary to retain such information since it can aid in establishing patterns of criminal activity and can provide valuable leads for Federal and other law enforcement agencies.

(5)(e)(2). To collect information to the greatest extent practicable from the subject individual in a criminal investigation or prosecution would present a serious impediment to law enforcement. The nature of criminal and other investigative activities is such that vital information about an individual can only be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(6) (e)(3). To provide individuals supplying information with a form stating the requirements

subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witness confidential informants.

(7)(e)(4) (G) and (H). These subsections are inapplicable to the extent that this system is exempt from the access provisions of subsection (d) and the rules provisions of subsection (e)(4)(I).

(8)(e)(4)(I). The categories of sources of the records in this system have been published in the *Federal Register* in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in this system, exemption from this provision is necessary to protect the confidentiality of the sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(9) (e)(5). In the collection of information for criminal law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance. Further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would inhibit the ability of trained investigators, intelligence analysts, and government attorneys in exercising their judgment in reporting on information and investigations and impede the development of criminal or other intelligence necessary for effective law enforcement.

(10)(e)(8). The individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.

(11)(f). This subsection is inapplicable to the extent that this system is exempt from the provisions of subsection (d).

(12)(g). Because some of the records in this system contain information which was compiled for law enforcement purposes and have been exempted from the access provisions of subsection (d), subsection (g) is inapplicable.

(s) The following system of records is exempted from 5 U.S.C. 552a(d).

Office of Special Investigations Displaced Persons Listings (JUSTICE/CRM-027).

This exemption applies to the extent that the records in this system are subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(t) Exemption from subsection (d) is justified for the following reasons:

(1) Access to records contained in this system could inform the subject of the identity of witnesses or informants. The release of such information could present a serious impediment to effective law enforcement by endangering the physical safety of witnesses or informants leading to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony; or by otherwise preventing the successful completion of an investigation.

(u) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(b)(1) and/or (k) from subsections (c)(3) and (4); (d)(1), (d)(2), (d)(3) and (d)(4); (e)(1), (e)(2), (e)(4)(G), (H) and (I), (e)(5) and (e)(8); (f), and (g) of 5 U.S.C. 552a: Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence Operations Center System (JUSTICE/CRM-028). These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j) and (k).

(v) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to provide the subject with an accounting of disclosed records in this system could inform that individual of the existence, nature, or scope of an actual or potential law enforcement or counterintelligence investigation by the Organized Crime Drug Enforcement Task Force Fusion Center, the International Organized Crime Intelligence and Operations Center, or the recipient agency, and could permit that individual to take measures to avoid detection or apprehension, to learn the identity of witnesses and informants or to destroy evidence, and would therefore present a serious impediment to law enforcement or counterintelligence efforts. In addition, disclosure of the accounting would amount to disclosure to the individual of the existence of a record. Moreover, release of an accounting may reveal information that is properly classified pursuant to Executive Order and could compromise national defense or foreign policy.

(2) From subsection (c)(4) because this subsection is inapplicable to the extent that an exemption is being claimed from subsections (d)(1), (2), (3), and (4).

(3) From subsection (d)(1) because disclosure of records in the system could alert the subject of an actual or potential criminal, civil, or regulatory investigation of the existence of that investigation, of the nature and scope of the information and evidence obtained as to his activities, of the identity of confidential witnesses and informants, of the investigative interest in the Organized Crime Drug Enforcement Task Force Fusion Center, International Organized Crime Intelligence and Operations Center, and other intelligence or law enforcement agencies (including those responsible for civil proceedings related to laws against drug trafficking, related financial crimes or international organized crime); lead to the destruction of evidence; improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; reveal the details of a sensitive investigative or intelligence technique, or the identity of a confidential source; or otherwise impede, compromise, or interfere with investigative efforts and other related law enforcement and/or intelligence activities. In addition, disclosure could invade the privacy of third parties and/or endanger the life, health, and physical safety of law enforcement personnel, confidential informants, witnesses, and potential crime victims. Access to records could also result in the release of information properly classified pursuant to Executive Order 13526, thereby compromising the national defense or foreign policy.

(4) From subsection (d)(2) because amendment of the records thought to be incorrect, irrelevant, or untimely would also interfere with ongoing investigations, criminal or civil law enforcement proceedings, and other law enforcement activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised, as well as impact information properly classified pursuant to Executive Order.

(5) From subsections (d)(3) and (4) because these subsections are inapplicable to the records for which exemption is claimed from (d)(1) and (2).

(6) From subsection (e)(1) because, in the course of its acquisition, collation, and analysis of information under the statutory authority granted to them, both the Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence and Operations Center will occasionally obtain information, including information properly classified pursuant to Executive Order, that concern actual or potential violations of law that are not strictly within its statutory or other authority or may compile information in the course of investigation which may not be relevant to a specific prosecution. It is impossible to determine in advance what information collected during an investigation will be important or crucial to the apprehension of fugitives. In the interests of effective law enforcement, it is necessary to

such information in this system of records because it can aid in establishing patterns of criminal activity and can provide valuable leads for federal and other law enforcement agencies. This consideration applies equally to information acquired from, or collated or analyzed for, both law enforcement agencies and agencies of the U.S. foreign intelligence community and military community.

(7) From subsection (e)(2) because in a criminal, civil, or regulatory investigation, prosecution, or proceeding, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation, prosecution, or proceeding would be placed on notice of the existence and nature of the investigation, prosecution, and proceeding and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony. Moreover, thorough and effective investigation and prosecution may require seeking information from a number of different sources.

(8) From subsection (e)(3) (to the extent applicable) because the requirement that individuals supplying information be provided a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants, endanger their lives, health, and physical safety. The individual could seriously interfere with undercover investigative techniques and could take appropriate steps to evade the investigation or flee a specific area.

(9) From subsections (e)(4)(G), (H) and (I) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(10) From subsection (e)(5) because the acquisition, collation, and analysis of information for law enforcement purposes from various agencies does not permit a determination in advance or a prediction of what information will be matched with other information and thus whether it is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant and untimely information may acquire new significance as further investigation brings new information to light and the accuracy of such information can often only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators, intelligence analysts, and government attorneys to exercise their judgment in collating and analyzing information and would impede the development of criminal or other intelligence necessary for effective law enforcement.

(11) From subsection (e)(8) because the individual notice requirements of subsection (e) could present a serious impediment to law enforcement by revealing investigative techniques, procedures, evidence, or interest and interfering with the ability to issue warrants or subpoenas, and could give persons sufficient warning to evade investigative efforts.

(12) From subsections (f) and (g) because these subsections are inapplicable to the extent the system is exempt from other specific subsections of the Privacy Act.

[Order No. 645–76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 659–76, 41 FR 32423, Aug. 3, 1976; Order No. 11–78, 43 FR 38386, Aug. 28, 1978; Order No. 30–79, 44 FR 54046, Sept. 18, 1979; Order Nos. 6–86, 7–86, 51 FR 15475, 15477, Apr. 24, 1986; Order No. 018–2004, 69 FR 72114, Dec. 13, 2004; Order No. 015–2006, 71 FR 58278, Oct. 3, 2006; Order No. 003–2009, 74 FR 42776, Aug. 25, 2009]

§ 16.92 Exemption of Environment and Natural Resources Division Systems—limited access.

(a)(1) The following system of records is exempted pursuant to 5 U.S.C. 552a(j)(2) from subsections (c)(3) and (4), (d), (e)(1), (e)(2), (e)(3), (e)(5), (e)(8), (f) and (g); in addition, the following systems of records are exempted pursuant to 5 U.S.C. 552a(k)(1) and (k)(2) from subsections (c)(3), (d), and (e)(1):

(i) Environment and Natural Resources Division Case and Related Files System, JUSTICE/ENRD–003.

(ii) [Reserved]

(2) These exemptions apply only to the extent that information in this system relates to a criminal investigation, prosecution or defense of actual or potential criminal or civil litigation, or which has been properly classified in the interest of national defense and foreign policy, and therefore is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1) and (k)(2). To the extent that information in a record pertaining to an individual does not relate to national defense or foreign policy, official Federal investigations, and/or law enforcement matters, the exemption does not apply. In addition, where compliance would not appear to interfere with or adversely affect the overall law or regulatory enforcement process, the applicable exemption may be waived by the Environment and Natural Resources Division.

(b) Only that information that relates to the investigation, prosecution or defense of actual or potential criminal or civil litigation, or which has been properly classified in the interest of national defense and foreign policy is exempted for the reasons set forth from the following subsections:

(1) *Subsection (c)(3)*. Subsection (c)(3) requires an agency to provide an accounting of disclosures of records concerning an individual. To provide the subject of a criminal or civil matter or case under investigation with an accounting of disclosures of records would inform that individual (and others to whom the subject might disclose the records) of the existence, nature, or scope of that investigation and thereby seriously impede law enforcement efforts by permitting the record subject and others to avoid criminal penalties and civil remedies.

(2) *Subsections (c)(4) (requiring an agency to inform individuals about any corrections made to a record that has been disclosed) and (g) (providing for civil remedies when an agency fails to comply with these provisions)*. These provisions are inapplicable to the extent that this system of records is exempted from subsection (d).

(3) *Subsection (d)*. Subsection (d) requires an agency to allow individuals to gain access to their record about him or herself; to dispute the accuracy, relevance, timeliness or completeness of such records; and to have an opportunity to amend his or her record or seek judicial review. To the extent that information contained in this system has been properly classified, relates to the investigation and/or prosecution of grand jury, civil fraud, and other law enforcement matters, disclosure could compromise matters which should be kept secret in the interest of national security or foreign policy; compromise confidential investigations or proceedings; impede affirmative enforcement actions based upon alleged violations of regulations or of civil or criminal laws; reveal the identity of confidential sources; and result in unwarranted invasion of the privacy of others. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) *Subsection (e)(1)*. Subsection (e)(1) requires an agency to maintain in its records only information about an individual that is relevant and necessary to accomplish the agency's purpose. In the course of criminal or civil investigations, cases, or other matters, the Environment and Natural Resources Division may obtain information concerning the actual or potential violation of laws which are not strictly within its statutory authority. In the interest of effective law enforcement, it is necessary to retain such information since it may establish

patterns of criminal activity or avoidance of other civil obligations and provide leads for F and other law enforcement agencies.

(5) *Subsection (e)(2)*. Subsection (e)(2) requires an agency to collect information to the greatest extent practicable from the subject individual when the information may result in adverse determinations about an individual's rights, benefits and privileges under Federal programs. To collect information from the subject of a criminal investigation or prosecution would present a serious impediment to law enforcement in that the subject (and others whom the subject might be in contact) would be informed of the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6) *Subsection (e)(3)*. Subsection (e)(3) requires an agency to inform each individual who asks to supply information, on a form that can be retained by the individual, the authority authorizes the solicitation, the principal purpose for the information, the routine uses of information, and the effects on the individual of not providing the requested information. To comply with this requirement during the course of a criminal investigation or prosecution would jeopardize the investigation by disclosing the existence of a confidential investigation, revealing the identity of witnesses or confidential informants, or impeding the information gathering process.

(7) *Subsection (e)(5)*. Subsection (e)(5) requires an agency to maintain records with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual. In compiling information for criminal law enforcement purposes, the accuracy, completeness, timeliness and relevancy of the information obtained cannot all be immediately determined. As new details of an investigation come to light, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can often only be determined in a court of law. Compliance with this requirement would therefore restrict the ability of government attorneys in exercising their judgment in developing information necessary for effective law enforcement.

(8) *Subsection (e)(8)*. Subsection (e)(8) requires agencies to make reasonable efforts to give notice to an individual when any record on the individual is made available to any person under compulsory legal process. To serve notice would give persons sufficient warning to evade law enforcement efforts.

(9) *Subsections (f) and (g)*. Subsection (f) requires an agency to establish procedures to

an individual to have access to information about him or herself and to contest information by an agency about him or herself. Subsection (g) provides for civil remedies against agencies who fail to comply with the Privacy Act requirements. These provisions are inapplicable to the extent that this system is exempt from the access and amendment provisions of subsection (c).

(c) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (d):

(1) Freedom of Information/Privacy Act Records System. (Justice/LDN-005).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c) (3) because that portion of the Freedom of Information/Privacy Act Records System that consists of investigatory materials compiled for law enforcement purposes is being exempted from access and contest; the provision for disclosure of accounting is applicable.

(2) From subsection (d) because of the need to safeguard the identity of confidential informants and avoid interference with ongoing investigations or law enforcement activities by preventing premature disclosure of information relating to those efforts.

[Order No. 688-77, 42 FR 10000, Feb. 18, 1977, as amended by Order No. 207-2000, 65 FR 75158, Dec. 1, 2000]

§ 16.93 Exemption of Tax Division Systems—limited access.

(a) The following systems of records are exempted pursuant to the provisions of 5 U.S.C. 552a (j)(2) from subsections (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f) and (g) of 5 U.S.C. 552a:

(1) Tax Division Central Classification Cards, Index Docket Cards, and Associated Records—Criminal Tax Cases (JUSTICE/TAX-001)—Limited Access.

(2) These exemptions apply to the extent that information in these systems is subject to

exemption pursuant to 5 U.S.C. 552a(j)(2).

(b) The system of records listed under paragraph (a)(1) of this section is exempted for the reasons set forth below, from the following provisions of 5 U.S.C. 552a:

(1)(c)(3). The release of the disclosure accounting, for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would enable the subject of an investigation of an actual or potential criminal tax case to determine whether he or she is the subject of investigation, to obtain valuable information concerning the nature of that investigation and the information obtained, and to determine the identity of witnesses or informants. Such access to investigative information would, accordingly, present a serious impediment to law enforcement. In addition, disclosure of the accounting would constitute notice to the individual of the existence of the record even though such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2)(c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records), this subsection is inapplicable to the extent that these systems of records are exempted from subsection (d).

(3) (d)(1); (d)(2); (d)(3); (d)(4). Access to the records contained in these systems would enable the subject of an actual or potential criminal tax investigation to determine the existence of that investigation, of the nature and scope of the information and evidence obtained as to his or her activities, and of the identity of witnesses or informants. Such access would, accordingly, provide information that could enable the subject to avoid detection, apprehension and prosecution. This result, therefore, would constitute a serious impediment to effective law enforcement not only because it would prevent the successful completion of the investigation but also because it could endanger the physical safety of witnesses or informants, lead to improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4)(e)(1). The notices for these systems of records published in the *Federal Register*, set forth the basic statutory or related authority for maintenance of these systems. However, in the course of criminal tax and related law enforcement investigations, cases, and matters, the Internal Revenue Service will occasionally obtain information concerning actual or potential violations of Internal Revenue Code provisions which may not be technically within its statutory or other authority or may compile information in the course of an investigation which may not be relevant to a specific prosecution. In the interest of effective law enforcement, it is necessary to retain some or all of such information in the

systems of records since it can aid in establishing patterns of criminal activity and can provide valuable leads for Federal and other law enforcement agencies.

(5)(e)(2). In a criminal tax investigation or prosecution, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, influence witnesses improperly, destroy evidence, or fabricate testimony.

(6)(e)(3). The requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(7)(e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Files) and (d) (Access to Records) of the Act these subsections are inapplicable to the extent these systems of records are exempted from subsection (f) and (d).

(8)(e)(4)(I). The categories of sources of the records in the systems have been published in the *Federal Register* in broad generic terms in the belief that this is all that subsection (e)(4) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from disclosure provision is necessary in order to protect the confidentiality of the sources of criminal tax related law enforcement information. Such exemption is further necessary to protect the lives and physical safety of witnesses and informants.

(9)(e)(5). In the collection of information for criminal tax enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. Furthermore, the accuracy of such information can often only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of government attorneys in exercising their judgment in reporting on information and investigations and impede the development of criminal tax information and related data necessary for effective law enforcement.

(10)(e)(8). The individual notice requirements of subsection (e)(8) could present a serious

impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.

(11)(f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an actual or potential criminal tax, civil tax, or regulatory investigation or prosecution must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation or prosecution pending or future. In addition, mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of investigation and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the requirements required pursuant to subsection (f) (2) through (5) are inapplicable to these systems of records to the extent that these systems of records are exempted from subsection (d).

(12)(g). Since an exemption is being claimed for subsections (d) (Access to Records) and (e) (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for subsections (d) and (e), to the extent that these systems of records are exempted from subsections (d) and (e).

(c) The following system of records is exempted pursuant to the provisions of 5 U.S.C. 552a(k)(2) from subsections (c)(3), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(4)(G), (e)(4)(H), and (f) of 5 U.S.C. 552a:

(1) Tax Division Central Classification Cards, Index Docket Cards, and Associated Records—Civil Tax Cases (JUSTICE/TAX-002)—Limited Access.

These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(d) The system of records listed under paragraph (c)(1) is exempted for the reasons set forth below, from the following provisions of 5 U.S.C. 552a:

(1)(c)(3). The release of the disclosure accounting, for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for

system of records, would enable the subject of an investigation of an actual or potential case to determine whether he or she is the subject of investigation, to obtain valuable information concerning the nature of that investigation and the information obtained, and determine the identity of witnesses or informants. Such access to investigative information would, accordingly, present a serious impediment to law enforcement. In addition, disclosure of the accounting would constitute notice to the individual of the existence of a record even though such notice requirement under subsection (f)(1) is specifically exempted for this system of records.

(2) (d)(1); (d)(2); (d)(3); (d)(4). Access to the records contained in this system would inform the subject of an actual or potential civil tax investigation of the existence of that investigation, the nature and scope of the information and evidence obtained as to his or her activities, and the identity of witnesses or informants. Such access would, accordingly, provide information that could enable the subject to avoid detection. This result, therefore, would constitute a serious impediment to effective law enforcement not only because it would prevent the successful completion of the investigation but also because it could endanger the physical safety of witnesses or informants, lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(3)(e)(1). The notices for this system of records published in the *Federal Register* set forth the basic statutory or related authority for maintenance of this system. However, in the course of civil tax and related law enforcement investigations, cases and matters, the Tax Division occasionally obtains information concerning actual or potential violations of law that are not strictly or technically within its statutory or other authority or may compile information in the course of an investigation which may not be relevant to a specific case. In the interests of effective law enforcement, it is necessary to retain some or all of such information in this system of records since it can aid in establishing patterns of tax compliance and can provide valuable leads for Federal and other law enforcement agencies.

(4)(e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Functions) and (d) (Access to Records) of the Act these subsections are inapplicable to the extent the system of records is exempted from subsection (f) and (d).

(5)(e)(4)(I). The categories of sources of the records in this system have been published in the *Federal Register* in broad generic terms in the belief that this is all that subsection (e)(4) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in this system, exemption from the

provision is necessary in order to protect the confidentiality of the sources of civil tax and related law enforcement information. Such exemption is further necessary to protect the and physical safety of witnesses and informants.

(6)(f). Procedures for notice to an individual pursuant to subsection (f)(1) as to existence records pertaining to the individual dealing with an actual or potential criminal tax, civil t regulatory investigation or prosecution must be exempted because such notice to an inc would be detrimental to the successful conduct and/or completion of an investigation or pending or future. In addition, mere notice of the fact of an investigation could inform th subject or others that their activities are under or may become the subject of an investig and could enable the subjects to avoid detection, to influence witnesses improperly, to evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) t required pursuant to subsection (f) (2) through (5) are inapplicable to this system of rec the extent that this system of records is exempted from subsection (d).

(e) The following system of records is exempt from subsections (c)(3) and (d)(1) of the F Act pursuant to 5 U.S.C. 552a(k)(5): Files of Applicants for Attorney and Non-Attorney F with the Tax Division, Justice/TAX-003. These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(k)(5).

(f) Exemption from the particular subsections is justified for the following reasons:

(1) From subsection (c)(3) because an accounting could reveal the identity of confidential sources and result in an unwarranted invasion of the privacy of others. Many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning an applicant for a position with the Tax Division. Disclosure of an accounting could reveal identity of a source of information and constitutes a breach of the promise of confidentiality to the Tax Division. This would result in the reduction in the free flow of information vital to determination of an applicant's qualifications and suitability for federal employment.

(2) From subsection (d)(1) because disclosure of records in the system could reveal the identity of confidential sources and result in an unwarranted invasion of the privacy of o Many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning an applicant for a Tax Division position. Access could reveal the of the source of the information and constitute a breach of the promise of confidentiality

part of the Tax Division. Such breaches ultimately would restrict the free flow of information vital to a determination of an applicant's qualifications and suitability.

[Order No. 742-77, 42 FR 40906, Aug. 12, 1977, as amended by Order No. 6-86, 51 FR 15478, Apr. 24, 1986; Order No. 003-2006, 71 FR 11309, Mar. 7, 2006]

§ 16.96 Exemption of Federal Bureau of Investigation Systems—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G) and (H), (e)(5), (e)(8), (f) and (g):

(1) Central Records System (CRS) (JUSTICE/FBI-002).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552(j) and (k). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, the applicable exemption may be waived by the FBI.

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting disclosures from records concerning him/her would reveal investigative interest by not only the FBI, but also by the recipient agency. This would permit the record subject to take appropriate measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, flee the area to avoid the thrust of the investigation.

(2)(i) From subsections (d), (e)(4) (G) and (H), (f) and (g) because these provisions concerning individual access to investigative records, compliance with which could compromise sensitive information classified in the interest of national security, interfere with the overall law enforcement process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety of law enforcement personnel.

(ii) Also, individual access to non-criminal investigative records, e.g., civil investigations and administrative inquiries, as described in subsection (k) of the Privacy Act, could also

compromise classified information related to national security, interfere with a pending investigation or internal inquiry, constitute an unwarranted invasion of privacy, reveal a confidential source or sensitive investigative technique, or pose a potential threat to law enforcement personnel. In addition, disclosure of information collected pursuant to an employment suitability or similar inquiry could reveal the identity of a source who provided information under an express promise of confidentiality, or could compromise the object fairness of a testing or examination process.

(iii) In addition, from paragraph (d)(2) of this section, because to require the FBI to amend information thought to be incorrect, irrelevant or untimely, because of the nature of the information collected and the essential length of time it is maintained, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to resolve questions of accuracy, etc.

(3) From subsection (e)(1) because:

(i) It is not possible in all instances to determine relevancy or necessity of specific information in the early stages of a criminal or other investigation.

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity in a specific investigative activity be established.

(iii) In any investigation the FBI might obtain information concerning violations of law not in its jurisdiction, but in the interest of effective law enforcement, dissemination will be made by the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or to another investigative activity under the jurisdiction of another agency.

(4) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual can only be obtained from other persons familiar with such individual and his/her activities. In such investigations it is not feasible

upon information furnished by the individual concerning his own activities.

(5) From subsection (e)(3) because disclosure would provide the subject with substantial information which could impede or compromise the investigation. The individual could so interfere with undercover investigative activities and could take appropriate steps to evade investigation or flee a specific area.

(6) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restriction imposed by subsection (e)(5) would limit the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement. In addition, because many of these records come from other federal, state, local, joint, foreign, tribal, and international agencies, it is administratively impossible to ensure compliance with this provision.

(7) From subsection (e)(8) because the notice requirements of this provision could seriously interfere with a law enforcement activity by alerting the subject of a criminal or other investigation of existing investigative interest.

(c) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), (g) and (m):

(1) Electronic Surveillance (Elsur) Indices (JUSTICE/FBI-006).

These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of accounting disclosures would place the subject of an investigation on notice that he is under investigation and provide him with significant information concerning the nature of the investigation, resulting in a serious impediment to law enforcement.

(2) From subsections (c)(4), (d), (e)(4) (G) and (H), and (g) because these provisions cover

an individual's access to records which concern him and such access to records in this would compromise ongoing investigations, reveal investigatory techniques and confidential informants, and invade the privacy of private citizens who provide information in connection with a particular investigation.

(3) From subsection (e)(1) because these indices must be maintained in order to provide information as described in the "routine uses" of this particular system.

(4) From subsections (e) (2) and (3) because compliance is not feasible given the subject matter of the indices.

(5) From subsection (e)(5) because this provision is not applicable to the indices in view of the "routine uses" of the indices. For example, it is impossible to predict when it will be necessary to utilize information in the system and, accordingly it is not possible to determine when records are timely.

(6) From subsection (e)(8) because the notice requirement could present a serious impediment to law enforcement by revealing investigative techniques, procedures and the existence of confidential investigations.

(7) From subsection (m) for the reasons stated in subsection (b)(7) of this section.

(e) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) and (3), (e)(4) (G) and (H), (e) (5) and (8), (f), and (g):

(1) Identification Division Records System (JUSTICE/FBI-009).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j).

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) for the reasons stated in subsection (d)(1) of this section.

(2) From subsections (c)(4), (d), (e)(4) (G) and (H), (f) and (g) because these provisions concern an individual's access to records which concern him. Such access is directed at

allowing the subject of a record to correct inaccuracies in it. Although an alternate system access has been provided in 28 CFR 16.30 to 34 and 28 CFR 20.34, the vast majority of records in this system concern local arrests which it would be inappropriate for the FBI to undertake to correct.

(3) From subsection (e)(1) because it is impossible to state with any degree of certainty information on these records is relevant to accomplish a purpose of the FBI, even though acquisition of the records from state and local law enforcement agencies is based on a statutory requirement. In view of the number of records in the system it is impossible to determine their relevancy.

(4) From subsection (e)(2) because the records in the system are necessarily furnished to criminal justice agencies due to their very nature.

(5) From subsection (e)(3) because compliance is not feasible due to the nature of the records.

(6) From subsection (e)(5) because the vast majority of these records come from local criminal justice agencies and it is administratively impossible to ensure that the records comply with this provision. Submitting agencies are, however, urged on a continuing basis to ensure that the records are accurate and include all dispositions.

(7) From subsection (e)(8) because the FBI has no logical manner to ascertain whether information has been made public and compliance with this provision would in any case, present an impediment to law enforcement by interfering with the ability to issue warrants or subpoenas and by revealing investigative techniques, procedures or evidence.

(g) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (4), (d), (e)(2), (e)(3), (e)(4)(G) and (H), (e)(5), (e)(8), (f), and (g):

(1) National Crime Information Center (NCIC) (JUSTICE/FBI-001). These exemptions apply to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(3).

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) for the reasons stated in subsection (d)(1) of this section.

(2) From subsections (c)(4), (d), (e)(4) (G) and (H), and (g) for the reasons stated in subsection (d)(2) of this section. When records are properly subject to access by the individual, an alternate means of access is provided in subsection (i) of this section.

(3) From subsection (e)(1) because information contained in this system is primarily from federal and local records, and it is for the official use of agencies outside the Federal Government in accordance with 28 U.S.C. 534.

(4) From subsections (e) (2) and (3) because it is not feasible to comply with these provisions given the nature of this system.

(5) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by subsection (e)(5) would limit the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement. In addition, the vast majority of these records come from other federal, state, local, joint, foreign, tribal, and international agencies and it is administratively impossible to ensure that the records comply with this provision. Submitting agencies are, however, urged on a continuing basis to ensure that the records are accurate and include all dispositions.

(6) From subsection (e)(8) for the reasons stated in subsection (d)(6) of this section.

(i) Access to computerized criminal history records in the National Crime Information Center is available to the individual who is the subject of the record pursuant to procedures and requirements specified in the Notice of Systems of Records compiled by the National Archives and Records Service and published under the designation:

(j) The following system of records is exempt from 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4) and (H), (e)(5), (f) and (g):

(1) National Center for the Analysis of Violent Crime (NCAVC) (JUSTICE/FBI-015).

These exemptions apply only to the extent that information in this system is subject to

exemption pursuant to 5 U.S.C. 552a (j)(2) and (k)(2).

(k) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because providing the accounting of disclosures to the subject could prematurely reveal investigative interest by the FBI and other law enforcement agencies thereby providing the individual an opportunity to impede an active investigation, destroy or alter evidence, and possibly render harm to violent crime victims and/or witnesses.

(2) From subsections (d), (e)(4) (G) and (H), and (f) because disclosure to the subject could interfere with enforcement proceedings of a criminal justice agency, reveal the identity of a confidential source, result in an unwarranted invasion of another's privacy, reveal the details of a sensitive investigative technique, or endanger the life and safety of law enforcement personnel, potential violent crime victims, and witnesses. Disclosure also could prevent future apprehension of a violent or exceptionally dangerous criminal fugitive should he or she modify his or her method of operation in order to evade law enforcement. Also, specifically subsection (d)(2), which permits an individual to request amendment of a record, because of the nature of the information in the system is such that an individual criminal offender would frequently demand amendment of derogatory information, forcing the FBI to continuously retrograde its criminal investigations in an attempt to resolve questions of accuracy, etc.

(3) From subsection (g) because the system is exempt from the access and amendment provisions of subsection (d).

(4) From subsection (e)(1) because it is not always possible to establish relevance and necessity of the information at the time it is obtained or developed. Information, the relevance and necessity of which may not be readily apparent, frequently can prove to be of investigative value at a later date and time.

(5) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restriction imposed by subsection (e)(5) would limit the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement. In addition, because many of these records come from other federal, state, local, joint, foreign, tribal, and international

agencies, it is administratively impossible to ensure compliance with this provision.

(l) The following system of records is exempt from 5 U.S.C. 552a (c)(3), (c)(4), (d), (e) (1 and (3), (e)(4) (G) and (H), (e)(5), (e)(8), (f) and (g).

(1) FBI Counterdrug Information Indices System (CIIS) (JUSTICE/FBI—016)

(2) [Reserved]

(m) These exemptions apply only to the extent that information in this system is subject exemption pursuant to 5 U.S.C. 552a (j)(2). Exemptions from the particular subsections justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting disclosures from records concerning him/her would reveal investigative interest by not only the FBI, but also by the recipient agency. This would permit the record subject to take appropriate measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, flee the area to avoid the thrust of the investigation.

(2) From subsection (c)(4) to the extent it is not applicable because an exemption is being claimed from subsection (d).

(3)(i) From subsections (d), (e)(4) (G) and (H) because these provisions concern individual access to records, compliance with which could compromise sensitive information, interfere with the overall law enforcement process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety of law enforcement personnel.

(ii) In addition, from paragraph (d), because to require the FBI to amend information that may be incorrect, irrelevant or untimely, because of the nature of the information collected and the essential length of time it is maintained, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to resolve questions of accuracy, etc.

(4)(i) From subsection (e)(1) because it is not possible in all instances to determine rele

or necessity of specific information in the early stages of a criminal or other investigation

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant necessary when collected ultimately may be deemed otherwise. It is only after the information is assessed that its relevancy and necessity in a specified investigative activity can be established.

(iii) In any investigation the FBI might obtain information concerning violations of law not within its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or to a specific investigative activity under the jurisdiction of another agency.

(5) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual often can only be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to principally rely upon information furnished by the individual concerning his or her activities.

(6) From subsection (e)(3) because disclosure would provide the subject with information which could impede or compromise the investigation. The individual could seriously interfere with undercover investigative activities and could take appropriate steps to evade the investigation or flee a specific area.

(7) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restriction imposed by subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(8) From subsection (e)(8) because the notice requirements of this provision could seriously

interfere with a law enforcement activity by alerting the subject of a criminal or other investigation of existing investigative interest.

(9) From subsection (f) to the extent that this system is exempt from the provisions of subsection (d).

(10) From subsection (g) to the extent that this system of records is exempt from the provisions of subsection (d).

(n) The following system of records is exempt from 5 U.S.C. 552a (c) (3) and (4); (d); (e) (2), and 3; (e)(4) (G) and (H); (e) (5) and (8); and (g):

(1) National DNA Index System (NDIS) (JUSTICE/FBI-017).

(2) [Reserved]

(o) These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available the accounting of disclosures of records to the subject of the record would prematurely place the subject on notice of the investigative interest of law enforcement agencies, provide the subject with significant information concerning the nature of the investigation, or permit the subject to take measures to impede the investigation (e.g., destroy or alter evidence, intimidate potential witnesses, or flee the country to avoid investigation and prosecution), and result in a serious impediment to law enforcement.

(2)(i) From subsections (c)(4), (d), (e)(4) (G) and (H), and (g) because these provisions concern an individual's access to records which concern him/her and access to records in this system would compromise ongoing investigations. Such access is directed at allowing the subject of the record to correct inaccuracies in it. The vast majority of records in this system are from the DNA records of local and State NDIS agencies which would be inappropriate and not feasible for the FBI to undertake to correct. Nevertheless, an alternate method to access, amend, and delete records in this system is available to an individual who is the subject of a record pursuant to procedures and requirements specified in the Notice of Systems of Records compiled by the National Archives and Records Administration and published in the *Federal Register*.

Register under the designation: National DNA Index System (NDIS) (JUSTICE/FBI-017)

(ii) In addition, from paragraph (d)(2) of this section, because to require the FBI to amend information thought to be incorrect, irrelevant, or untimely, because of the nature of the information collected and the essential length of time it is maintained, would create an impossible administrative and investigative burden by forcing the agency to continuous retrograde investigations attempting to resolve questions of accuracy, etc.

(iii) In addition, from subsection (g) to the extent that the system is exempt from the amendment provisions of subsection (d).

(3) From subsection (e)(1) because:

(i) Information in this system is primarily from State and local records and it is for the off use of agencies outside the Federal Government.

(ii) It is not possible in all instances to determine the relevancy or necessity of specific information in the early stages of the criminal investigative process.

(iii) Relevance and necessity are questions of judgment and timing; what appears relevant necessary when collected ultimately may be deemed unnecessary, and vice versa. It is after the information is assessed that its relevancy in a specific investigative activity can be established.

(iv) Although the investigative process could leave in doubt the relevancy and necessity of evidence which had been properly obtained, the same information could be relevant to an investigation or investigative activity under the jurisdiction of the FBI or another law enforcement agency.

(4) From subsections (e)(2) and (3) because it is not feasible to comply with these provisions given the nature of this system. Most of the records in this system are necessarily furnished by State and local criminal justice agencies and not by individuals due to the very nature of the records and the system.

(5) From subsection (e)(5) because the vast majority of these records come from State and local criminal justice agencies and because it is administratively impossible for them and

FBI to insure that the records comply with this provision. Submitting agencies are urged make every effort to insure records are accurate and complete; however, since it is not possible to predict when information in the indexes of the system (whether submitted by State or criminal justice agencies or generated by the FBI) will be matched with other information, it is not possible to determine when most of them are relevant or timely.

(6) From subsection (e)(8) because the FBI has no logical manner to determine when a process has been made public and compliance with this provision would provide an impediment to law enforcement by interfering with ongoing investigations.

(p) The National Instant Criminal Background Check System (NICS), (JUSTICE/FBI-018 Privacy Act system of records, is exempt:

(1) Pursuant to 5 U.S.C. 552a(j)(2), from subsections (c) (3) and (4); (d); (e) (1), (2) and (e)(4) (G) and (H); (e) (5) and (8); and (g); and

(2) Pursuant to 5 U.S.C. 552a(k) (2) and (3), from subsections (c)(3), (d), (e)(1), and (e) and (H).

(q) These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(2), and (k)(3). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the accounting of disclosures would place the subject on notice that the subject is or has been the subject of investigation and result in a serious impediment to law enforcement.

(2) From subsection (c)(4) to the extent that it is not applicable since an exemption is claimed from subsection (d).

(3)(i) From subsections (d) and (e)(4) (G) and (H) because these provisions concern an individual's access to records which concern the individual and such access to records system would compromise ongoing investigations, reveal investigatory techniques and confidential informants, invade the privacy of persons who provide information in connection with a particular investigation, or constitute a potential danger to the health or safety of law enforcement personnel.

(ii) In addition, from subsection (d)(2) because, to require the FBI to amend information to be not accurate, timely, relevant, and complete, because of the nature of the information collected and the essential length of time it is maintained, would create an impossible administrative burden by forcing the agency to continuously update its investigations attempting to resolve these issues.

(iii) Although the Attorney General is exempting this system from subsections (d) and (e) and (H), an alternate method of access and correction has been provided in 28 CFR, part 25, subpart A.

(4) From subsection (e)(1) because it is impossible to state with any degree of certainty information in these records is relevant to accomplish a purpose of the FBI, even though acquisition of the records from state and local law enforcement agencies is based on a statutory requirement. In view of the number of records in the system, it is impossible to search them for relevancy.

(5) From subsections (e) (2) and (3) because the purpose of the system is to verify information about an individual. It would not be realistic to rely on information provided by the individual. In addition, much of the information contained in or checked by this system is from Federal, State, and local criminal history records.

(6) From subsection (e)(5) because it is impossible to predict when it will be necessary to review the information in the system, and, accordingly, it is not possible to determine in advance when the records will be timely. Since most of the records are from State and local or other Federal agency records, it would be impossible to review all of them to verify that they are accurate. In addition, an alternate procedure is being established in 28 CFR, part 25, subpart A, so that records can be amended if found to be incorrect.

(7) From subsection (e)(8) because the notice requirement could present a serious impediment to law enforcement by revealing investigative techniques and confidential investigations.

(8) From subsection (g) to the extent that, pursuant to subsections (j)(2), (k)(2), and (k)(3), this system is exempted from the other subsections listed in paragraph (p) of this section.

(r) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), and (4); (e)(1), (2), (3), (5), and (8); and (g):

(1) Terrorist Screening Records System (TSRS) (JUSTICE/FBI-019).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). Where compliance would appear to interfere with or adversely affect the counterterrorism purposes of this system or the overall law enforcement process, the applicable exemption may be waived by the FOIA officer at the sole discretion.

(s) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting disclosures from records concerning him/her would specifically reveal any investigative information in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or suspected terrorist by notifying the record subject that he/she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, flee the area to avoid or impede the investigation. Similarly, disclosing this information to individuals who have been misidentified as known or suspected terrorists due to a close similarity could reveal the Government's investigative interest in a terrorist suspect, because it could make known the name of the individual who actually is the subject of the Government's interest. Consequently, the Government has as great an interest in protecting the confidentiality of identifying information of misidentified persons as it does in protecting the confidentiality of the identities of known or suspected terrorists.

(2) From subsection (c)(4) because this system is exempt from the access and amendment provisions of subsection (d).

(3) From subsections (d)(1), (2), (3), and (4) because these provisions concern individual access to and amendment of records contained in this system, which consists of counterterrorism, investigatory and intelligence records. Compliance with these provisions could alert the subject of a terrorism investigation of the fact and nature of the investigation and/or the investigative interest of the FBI and/or other intelligence or law enforcement agencies; compromise sensitive information classified in the interest of national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; or identify a confidential source or disclose information which would constitute an unwarranted

invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing counterterrorism investigations and analysis activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised. Similarly, compliance with these provisions with respect to records on individuals who have been misidentified as known or suspected terrorists due to a clerical name similarity could reveal the Government's investigative interest in a terrorist suspect because it could make known the name of the individual who actually is the subject of the Government's interest.

(4) From subsection (e)(1) because it is not always possible for TSC to know in advance what information is relevant and necessary for it to complete an identity comparison between an individual being screened and a known or suspected terrorist. Also, because TSC and the FBI may not always know what information about an encounter with a known or suspected terrorist will be relevant to law enforcement for the purpose of conducting an operational response.

(5) From subsection (e)(2) because application of this provision could present a serious impediment to counterterrorism efforts in that it would put the subject of an investigation or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(6) From subsection (e)(3), to the extent that this subsection is interpreted to require TSC to provide notice to an individual if TSC receives information about that individual from a third party. Should the subsection be so interpreted, exemption from this provision is necessary to avoid impeding counterterrorism efforts by putting the subject of an investigation, study, or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede that activity.

(7) From subsection (e)(5) because many of the records in this system are derived from domestic and foreign agency record systems and therefore it is not possible for the FBI or TSC to vouch for their compliance with this provision; however, the TSC has implemented internal quality assurance procedures to ensure that TSC terrorist screening data is as thorough, accurate, and current as possible. In addition, TSC supports but does not control

investigations; therefore, it must be able to collect information related to terrorist identities and encounters for distribution to law enforcement and intelligence agencies that do conduct terrorism investigations. In the collection of information for law enforcement, counterterrorism, and intelligence purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant untimely information may acquire new significance as further investigation brings new light. The restrictions imposed by (e)(5) would limit the ability of those agencies' trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts. The TSC has, however, implemented internal quality assurance procedures to ensure that TSC terrorist screening data is as thorough, accurate, and complete as possible. The FBI also is exempting the TSRS from the requirements of subsection (e)(5) in order to prevent the use of a challenge under subsection (e)(5) as a collateral means to gain access to records in the TSRS. The FBI has exempted TSRS records from the access and amendment requirements of subsection (d) of the Privacy Act in order to protect the integrity of counterterrorism investigations. Exempting the TSRS from subsection (e)(5) serves to prevent the assertion of challenges to a record's accuracy, timeliness, completeness, and/or reliability under subsection (e)(5) to circumvent the exemption claimed from subsection (d).

(8) From subsection (e)(8) because to require individual notice of disclosure of information to compulsory legal process would pose an impossible administrative burden on the FBI, the TSC and could alert the subjects of counterterrorism, law enforcement, or intelligence investigations to the fact of those investigations when not previously known.

(9) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

(t) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), and (4); (e)(1), (2), (3), (5) and (8); and (g) of the Privacy Act:

(1) Law Enforcement National Data Exchange (N-DEx), (JUSTICE/FBI-020).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system, or the overall law enforcement process, the applicable exemption may be waived by the FBI in its sole discretion.

(u) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because this system is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures from records concerning him/her would specifically reveal any investigative in the individual. Revealing this information may thus compromise ongoing law enforcer efforts. Revealing this information may also permit the record subject to take measures impede the investigation, such as destroying evidence, intimidating potential witnesses fleeing the area to avoid the investigation.

(2) From subsection (c)(4) because this system is exempt from the access and amendr provisions of subsection (d).

(3) From subsections (d)(1), (2), (3), and (4), because these provisions concern individu access to and amendment of investigatory records, compliance with which could alert th subject of an investigation of the fact and nature of the investigation, and/or the investig interest of the FBI and other law enforcement agencies; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; possibly identify a confic source or disclose information which would constitute an unwarranted invasion of anoth personal privacy; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential inform and witnesses. Amendment of these records would interfere with ongoing investigations other law enforcement activities and impose an impossible administrative burden by req investigations, analyses, and reports to be continuously reinvestigated and revised.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement purposes and, in fact, a major of the N-DEx information sharing system is that the relevance of certain information may always be evident in the absence of the ability to correlate that information with other ex law enforcement data.

(5) From subsection (e)(2) because application of this provision could present a serious impediment to efforts to solve crimes and improve homeland security in that it would pu subject of an investigation on notice of that fact, thereby permitting the subject to engag conduct intended to frustrate or impede that activity.

(6) From subsection (e)(3) because disclosure would put the subject of an investigation notice of that fact and would permit the subject to engage in conduct intended to thwart activity.

(7)(i) From subsection (e)(5) because many of the records in this system are records contributed by other agencies and the restrictions imposed by (e)(5) would limit the utility of the N-DEx system. All data contributors are expected to ensure that information they share is relevant, timely, complete and accurate. In fact, rules for use of the N-DEx system will require that information be updated periodically and not be used as a basis for action or dissemination beyond the recipient without the recipient first obtaining permission from the record owner/contributor. These rules will be enforced through robust audit procedures. The effect of these rules should ameliorate any perceived concerns about the integrity of the information in the N-DEx system. Nevertheless, exemption from this provision is warranted in order to reduce the administrative burden on the FBI to vouch for compliance with the provision on N-DEx data contributors and to encourage those contributors to share information the significance of which may only become apparent when combined with other information in the N-DEx system.

(ii) The FBI is also exempting the N-DEx from subsection (e)(5) in order to block the use of a challenge under subsection (e)(5) as a collateral means to obtain access to records in the N-DEx. The FBI has exempted these records from the access and amendment requirements of subsection (d) of the Privacy Act in order to protect the integrity of law enforcement investigations. Exempting the N-DEx system from subsection (e)(5) complements this exemption and will provide the FBI with the ability to prevent the assertion of challenges to a record's accuracy, timeliness, completeness and/or relevance under subsection (e)(5) to circumvent the exemption claimed from subsection (d).

(8) From subsection (e)(8), because to require individual notice of disclosure of information to compulsory legal process would pose an impossible administrative burden on the FBI and may alert the subjects of law enforcement investigations to the fact of those investigations when not previously known.

(9) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

[Order No. 40-80, 45 FR 5301, Jan. 23, 1980, as amended by Order No. 64-81, 46 FR

Apr. 6, 1981; Order No. 63–81, 46 FR 22362, Apr. 17, 1981; Order No. 67–81, 46 FR 30 June 9, 1981; Order No. 15–85, 50 FR 31361, Aug. 2, 1985; Order No. 6–86, 51 FR 154 24, 1986; Order No. 94–94, 59 FR 47081, Sept. 14, 1994; Order No. 124–96, 61 FR 651 Dec. 11, 1996; Order No. 155–98, 63 FR 65062, Nov. 25, 1998; Order No. 010–2003, 68 14140, Mar. 24, 2003; Order No. 010–2005, 70 FR 72204, Dec. 2, 2005; Order No. 001– 73 FR 9947, Feb. 25, 2008]

§ 16.97 Exemption of Bureau of Prisons Systems—limited access.

(a) The following systems of records are exempt from 5 U.S.C. 552a (c) (3) and (4), (d), and (3), (e)(4) (H), (e)(8), (f) and (g):

- (1) Custodial and Security Record System (JUSTICE/BOP–001).
- (2) Industrial Inmate Employment Record System (JUSTICE/BOP–003).
- (3) Inmate Administrative Remedy Record System (JUSTICE/BOP–004).
- (4) Inmate Central Record System (JUSTICE/BOP–005).
- (5) Inmate Commissary Accounts Record System (JUSTICE/BOP–006).
- (6) Inmate Physical and Mental Health Record System (JUSTICE/BOP–007).
- (7) Inmate Safety and Accident Compensation Record System (JUSTICE/BOP–008).
- (8) Federal Tort Claims Act Record System (JUSTICE/BOP–009).

These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(j).

(b) Exemptions from the particular subsections are justified for the following reasons:

- (1) From subsection (c)(3) because inmates will not be permitted to gain access or to see contents of these record systems under the provisions of subsection (d) of 5 U.S.C. 552. Revealing disclosure accountings can compromise legitimate law enforcement activities

Bureau of Prisons responsibilities.

(2) From subsection (c)(4) because exemption from provisions of subsection (d) will make notification of formal disputes inapplicable.

(3) From subsection (d) because exemption from this subsection is essential to protect the processes by which Bureau personnel are able to formulate decisions and policies with respect to federal prisoners, to prevent disclosure of information to federal inmates that would jeopardize legitimate correctional interests of security, custody, or rehabilitation, and to receipt of relevant information from other federal agencies, state and local law enforcement agencies, and federal and state probation and judicial offices.

(4) From subsection (e)(2) because primary collection of information directly from federal inmates about criminal sentences or criminal records is highly impractical and inappropriate.

(5) From subsection (e)(3) because in view of the Bureau of Prisons' responsibilities, application of this provision to its operations and collection of information is inappropriate.

(6) From subsection (e)(4)(H) because exemption from provisions of subsection (d) will make publication of agency procedures under this subsection inapplicable.

(7) From subsection (e)(8) because the nature of Bureau of Prisons law enforcement activities renders notice of compliance with compulsory legal process impractical.

(8) From subsection (f) because exemption from provisions of subsection (d) will render compliance with provisions of this subsection inapplicable.

(9) From subsection (g) because exemption from provisions of subsection (d) will render provisions of this subsection inapplicable.

(c) The following system of records is exempted pursuant to 5 U.S.C. 552a(j)(2) from subsections (c)(3) and (4), (d), (e)(1), (2) and (3), (e)(5) and (e)(8), and (g). In addition, the following system of records is exempted pursuant to 5 U.S.C. 552a(k)(2) from subsections (c)(3), (d), and (e)(1):

Bureau of Prisons Access Control Entry/Exit, (JUSTICE/BOP-010).

(d) These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) or (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, e.g., public source materials, or those supplied by third parties, the applicable exemption may be waived, either partially or totally, by the BOP. Exemptions from the particular subsection are justified for the following reasons:

(1) From subsection (c)(3) for similar reasons as those enumerated in paragraph (3).

(2) From subsection (c)(4) to the extent that exemption from subsection (d) will make notification of corrections or notations of disputes inapplicable.

(3) From the access provisions of subsection (d) to the extent that exemption from this subsection may appear to be necessary to prevent access by record subjects to information that may jeopardize the legitimate correctional interests of safety, security, and good order in Bureau of Prisons facilities; to protect the privacy of third parties; and to protect access to relevant information received from third parties, such as other Federal, State, local and foreign law enforcement agencies, Federal and State probation and judicial offices, the disclosure of which may permit a record subject to evade apprehension, prosecution, etc.; and/or to otherwise protect investigatory or law enforcement information, whether received from other third parties, or whether developed internally by the BOP.

(4) From the amendment provisions of subsection (d) because amendment of the records would interfere with law enforcement operations and impose an impossible administrative burden. In addition to efforts to ensure accuracy so as to withstand possible judicial scrutiny, it would require that law enforcement and investigatory information be continuously reexamined even where the information may have been collected from the record subject. Also, where records are provided by other Federal criminal justice agencies or other State, local and foreign jurisdictions, it may be administratively impossible to ensure compliance with this provision.

(5) From subsection (e)(1) to the extent that the BOP may collect information that may be relevant to the law enforcement operations of other agencies. In the interests of overall, effective law enforcement, such information should be retained and made available to the agencies with relevant responsibilities.

(6) From subsection (e)(2) because primary collection of information directly from the re subject is often highly impractical, inappropriate and could result in inaccurate informati

(7) From subsection (e)(3) because compliance with this subsection may impede the co of information that may be valuable to law enforcement interests.

(8) From subsection (e)(5) because in the collection and maintenance of information for enforcement purposes, it is impossible to determine in advance what information is accu relevant, timely and complete. Data which may seem unrelated, irrelevant or incomplete collected may take on added meaning or significance as an investigation progresses or the passage of time, and could be relevant to future law enforcement decisions.

(9) From subsection (e)(8) because the nature of BOP law enforcement activities render notice of compliance with compulsory legal process impractical and could seriously jeop institution security and personal safety and/or impede overall law enforcement efforts.

(10) From subsection (g) to the extent that the system is exempted from subsection (d).

(e) The following system of records is exempt from 5 U.S.C. 552a (c) (3) and (4), (d), (e) and (3), (e)(5) and (e)(8), (f) and (g):

Telephone Activity Record System (JUSTICE/BOP-011).

(f) These exemptions apply only to the extent that information in this system is subject t exemption pursuant to 5 U.S.C. 552a (j)(2) and/or (k)(2). Where compliance would not a to interfere with or adversely affect the law enforcement process, and/or where it may b appropriate to permit individuals to contest the accuracy of the information collected, th applicable exemption may be waived, either partially or totally, by the BOP. Exemptions the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) to the extent that this system of records is exempt from subs (d), and for such reasons as those cited for subsection (d) in paragraph (f)(3) below.

(2) From subsection (c)(4) to the extent that exemption from subsection (d) makes this exemption inapplicable.

(3) From the access provisions of subsection (d) because exemption from this subsection is essential to prevent access of information by record subjects that may invade third party privacy; frustrate the investigative process; jeopardize the legitimate correctional interest in safety, security, and good order to prison facilities; or otherwise compromise, impede, or interfere with BOP or other law enforcement agency activities.

(4) From the amendment provisions from subsection (d) because amendment of the record may interfere with law enforcement operations and would impose an impossible administrative burden by requiring that, in addition to efforts to ensure accuracy so as to withstand potential judicial scrutiny, it would require that law enforcement information be continuously reexamined even where the information may have been collected from the record subject. Also, some of these records come from other Federal criminal justice agencies or State, local and foreign jurisdictions, or from Federal and State probation and judicial offices, and it is administratively impossible to ensure that the records comply with this provision.

(5) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual can be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely solely upon information furnished by the individual concerning his/her own activities since this may result in inaccurate information.

(6) From subsection (e)(3) because in view of BOP's operational responsibilities, application of this provision to the collection of information is inappropriate. Application of this provision to provide the subject with substantial information which may in fact impede the information gathering process or compromise an investigation.

(7) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Material which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance at a later date or as an investigation progresses. Also, some of these records may come from other Federal, State, local and foreign law enforcement agencies, and from Federal and State probation and judicial offices and it is administratively impossible to ensure that the records comply with this provision. It would also require that law enforcement information be continuously reexamined even where the information may have been collected from the record subject.

(8) From subsection (e)(8) because the nature of BOP law enforcement activities render impractical the notice of compliance with compulsory legal process. This requirement could present a serious impediment to law enforcement such as revealing investigative techniques, the existence of confidential investigations, jeopardize the security of third parties, or otherwise compromise law enforcement efforts.

(9)–(10) [Reserved]

(11) From subsections (f) and (g) to the extent that this system is exempt from the accession and amendment provisions of subsection (d).

(g) The following system of records is exempt pursuant to the provisions of 5 U.S.C. 552a from subsections (c) (3) and (4), (d), (e) (1), (2), and (3), (e)(5) and (e)(8), and (g) of 5 U.S.C. 552a. In addition, the following system of records is exempt pursuant to the provisions of 5 U.S.C. 552a (k)(1) and (k)(2) from subsections (c)(3), (d), and (e)(1) of 5 U.S.C. 552a:

Bureau of Prisons, Office of Internal Affairs Investigative Records, JUSTICE/BOP–012

(h) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2). Where compliance would appear to interfere with or adversely affect the law enforcement process, and/or where it would be appropriate to permit individuals to contest the accuracy of the information collected, public source materials, the applicable exemption may be waived, either partially or totally, by the Office of Internal Affairs (OIA). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because release of disclosure accounting could alert the subjects of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation and the fact that they are subjects of the investigation, and reveal investigative interest by not only the OIA but also by the recipient agency. Since release of such information to the subjects of an investigation would provide them with significant information concerning the nature of the investigation, release could result in activities that would impede or compromise law enforcement such as: the destruction of documentary evidence; improper influencing of witnesses; endangerment of the physical safety of confidential sources, witnesses, and law enforcement personnel; fabrication of testimony; and flight of the subjects from the area. In addition, release of disclosure accounting could result in the release of

properly classified information which could compromise the national defense or disrupt policy.

(2) From subsection (c)(4) because this system is exempt from the access provisions of subsection (d) pursuant to subsections (j) and (k) of the Privacy Act.

(3) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could provide the subject of an investigation information concerning law enforcement activities such as that relating to an actual or potential criminal, civil or regulatory violation; the existence of an investigation; the nature and scope of the information and evidence obtained as to his activities; the identity of confidential sources, witnesses, and law enforcement personnel; and information that may enable the subject to avoid detection or apprehension. Such disclosure would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation, endanger the physical safety of confidential sources, witnesses, and law enforcement personnel; and/or lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony. In addition, granting access to such information could disclose security-sensitive or confidential business information or information that would constitute an unwarranted invasion of the personal privacy of third parties. Finally, access to the records could result in the release of properly classified information which could compromise the national defense or disrupt foreign policy. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because the application of this provision could impair investigations and interfere with the law enforcement responsibilities of the OIA for the following reasons:

(i) It is not possible to detect relevance or necessity of specific information in the early stages of a civil, criminal or other law enforcement investigation, case, or matter, including investigations in which use is made of properly classified information. Relevance and necessity are questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established.

(ii) During the course of any investigation, the OIA may obtain information concerning actual or potential violations of laws other than those within the scope of its jurisdiction. In the interest of effective law enforcement, the OIA should retain this information as it may aid in establishing patterns of criminal activity, and can provide valuable leads for Federal and other law

enforcement agencies.

(iii) In interviewing individuals or obtaining other forms of evidence during an investigation information may be supplied to an investigator which relates to matters incidental to the primary purpose of the investigation but which may relate also to matters under the investigative jurisdiction of another agency. Such information cannot readily be segrega

(5) From subsection (e)(2) because, in some instances, the application of this provision present a serious impediment to law enforcement for the following reasons:

(i) The subject of an investigation would be placed on notice as to the existence of an investigation and would therefore be able to avoid detection or apprehension, to improper influence witnesses, to destroy evidence, or to fabricate testimony.

(ii) In certain circumstances the subject of an investigation cannot be required to provide information to investigators, and information relating to a subject's illegal acts, violations rules of conduct, or any other misconduct must be obtained from other sources.

(iii) In any investigation it is necessary to obtain evidence from a variety of sources other the subject of the investigation in order to verify the evidence necessary for successful litigation.

(6) From subsection (e)(3) because the application of this provision would provide the s of an investigation with substantial information which could impede or compromise the investigation. Providing such notice to a subject of an investigation could interfere with a undercover investigation by revealing its existence, and could endanger the physical sa confidential sources, witnesses, and investigators by revealing their identities.

(7) From subsection (e)(5) because the application of this provision would prevent the collection of any data not shown to be accurate, relevant, timely, and complete at the m it is collected. In the collection of information for law enforcement purposes, it is imposs determine in advance what information is accurate, relevant, timely, and complete. Mate which may seem unrelated, irrelevant, or incomplete when collected may take on addec meaning or significance as an investigation progresses. The restrictions of this provision interfere with the preparation of a complete investigation report, and thereby impede eff law enforcement.

(8) From subsection (e)(8) because the application of this provision could prematurely reveal an ongoing criminal investigation to the subject of the investigation, and could reveal investigation techniques, procedures, and/or evidence.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j)(2), (k)(1), and (k)(2) Privacy Act.

(i) Consistent with the legislative purpose of the Privacy Act of 1974 (Pub. L. 93-579) the Bureau of Prisons has initiated a procedure whereby federal inmates in custody may gain access and review of their individual prison files maintained at the institution of incarceration. Access to these files is limited only to the extent that the disclosure of records to the inmate would jeopardize its decision-making or policy determinations essential to the effective operation of the Bureau of Prisons; to the extent that disclosure of the records to the inmate would jeopardize private rights of others, or a legitimate correctional interest of security, custody, or rehabilitation; to the extent information is furnished with a legitimate expectation of confidentiality. The Bureau of Prisons will continue to provide access to former inmates under existing regulations and policies consistent with the interests listed above. Under present Bureau of Prisons regulations, inmates in federal institutions may file administrative complaints on any subject under the control of the Bureau. This would include complaints pertaining to information contained in these systems of records.

(j) The following system of records is exempted pursuant to 5 U.S.C. 552a(j) from subsections (e)(1) and (e)(5): Bureau of Prisons Inmate Central Records System, (Justice/BOP-005)

(k) These exemptions apply only to the extent that information in this system is subject to an exemption pursuant to 5 U.S.C. 552a(j). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to allow individuals to contest the accuracy of the information collected, e.g. public source material, or those supplied by third parties, the applicable exemption may be waived, either partially or totally, by the Bureau. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (e)(1) to the extent that the Bureau may collect information that may be relevant to the law enforcement operations of other agencies. In the interests of overall, effective law enforcement, such information should be retained and made available to the

agencies with relevant responsibilities.

(2) From subsection (e)(5) because in the collection and maintenance of information for enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Data which may seem unrelated, irrelevant or incomplete collected may take on added meaning or significance during the course of an investigation with the passage of time, and could be relevant to future law enforcement decisions. In addition, because many of these records come from the courts and other state and local criminal justice agencies, it is administratively impossible for them and the Bureau to ensure compliance with this provision. The restrictions of subsection (e)(5) would restrict and distract trained correctional managers from timely exercising their judgment in managing the inmate population and providing for the safety and security of the prisons and the public.

(l) The following system of records is exempted pursuant to 5 U.S.C. 552a(j) from subsection (e)(1) and (e)(5): Bureau of Prisons Inmate Trust Fund Accounts and Commissary Record System, (Justice/BOP-006).

(m) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j). Where compliance would not appear to interfere or adversely affect the law enforcement process, and/or where it may be appropriate to allow individuals to contest the accuracy of the information collected, e.g. public source material, those supplied by third parties, the applicable exemption may be waived, either partially or totally, by the Bureau. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (e)(1) to the extent that the Bureau may collect information that may be relevant to the law enforcement operations of other agencies. In the interests of overall, effective law enforcement, such information should be retained and made available to those agencies with relevant responsibilities.

(2) From subsection (e)(5) because in the collection and maintenance of information for enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Data which may seem unrelated, irrelevant or incomplete collected may take on added meaning or significance as an investigation progresses or with the passage of time, and could be relevant to future law enforcement decisions. In addition, amendment of the records may interfere with law enforcement operations and would impose an impossible administrative burden by requiring that law enforcement information be

continuously reexamined, even where the information may have been collected from the subject or other criminal justice agencies. The restrictions of subsection (e)(5) would restrict and delay trained correctional managers from timely exercising their judgment in managing the inmate population and providing for the safety and security of the prisons and the public.

(n) The following system of records is exempted pursuant to 5 U.S.C. 552a(j) from subsections (e)(1) and (e)(5): Bureau of Prisons Inmate Physical and Mental Health Records System (Justice/BOP-007).

(o) These exemptions apply only to the extent that information in this system is subject to an exemption pursuant to 5 U.S.C. 552a(j). Where compliance would not appear to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to allow individuals to contest the accuracy of the information collected, e.g. public source material or those supplied by third parties, the applicable exemption may be waived, either partially or totally, by the Bureau. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (e)(1) to the extent that the Bureau may collect information that may be relevant to the law enforcement operations of other agencies. In the interests of overall, effective law enforcement, such information should be retained and made available to those agencies with relevant responsibilities.

(2) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Data which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance during the course of an investigation with the passage of time, and could be relevant to future law enforcement decisions. In addition, because many of these records come from sources outside the Bureau of Prisons it is administratively impossible for them and the Bureau to ensure compliance with this provision. The restrictions of subsection (e)(5) would restrict and delay trained correctional managers from timely exercising their judgment in managing the inmate population and providing for the health care of the inmates and the safety and security of the prisons and the public.

(p) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (4), (d)(1)–(3), (e)(2) and (3), (e)(5), and (g):

Inmate Electronic Message Record System (JUSTICE /BOP-013).

(q) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and/or (k)(2). Where compliance would not be expected to interfere with or adversely affect the law enforcement process, and/or where it may be appropriate to permit individuals to contest the accuracy of the information collected, the applicable exemption may be waived, either partially or totally, by the BOP. Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) to the extent that this system of records is exempt from subsection (d), and for such reasons as those cited for subsection (d) in paragraph (q)(3) below.

(2) From subsection (c)(4) to the extent that exemption from subsection (d) makes this exemption inapplicable.

(3) From the access provisions of subsection (d) because exemption from this subsection is essential to prevent access of information by record subjects that may invade third party privacy; frustrate the investigative process; jeopardize the legitimate correctional interest in safety, security and good order to prison facilities; or otherwise compromise, impede, or interfere with BOP or other law enforcement agency activities.

(4) From the amendment provisions of subsection (d) because amendment of the records would interfere with law enforcement operations and would impose an impossible administrative burden by requiring that, in addition to efforts to ensure accuracy so as to withstand potential judicial scrutiny, it would require that law enforcement information be continuously reexamined even where the information may have been collected from the record subject. Also, some of these records come from other Federal criminal justice agencies or State, local and foreign jurisdictions, or from Federal and State probation and judicial offices, and it is administratively impossible to ensure that records comply with this provision.

(5) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual can be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely solely upon information furnished by the individual concerning his/her own activities since this may result in inaccurate information and compromise ongoing criminal investigations or correctional management decisions.

(6) From subsection (e)(3) because in view of BOP's operational responsibilities, application of this provision to the collection of information is inappropriate. Application of this provision would provide the subject with substantial information which may in fact impede the information gathering process or compromise ongoing criminal investigations or correctional management decisions.

(7) From subsection (e)(5) because in the collection and maintenance of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely and complete. Material which may seem unrelated, irrelevant or incomplete when collected may take on added meaning or significance at a later date or as an investigation progresses. Also, some of these records may come from other Federal, State, local and foreign law enforcement agencies, and from Federal and State probation and parole offices and it is administratively impossible to ensure that the records comply with this provision. It would also require that law enforcement information be continuously reexamined even where the information may have been collected from the record subject.

(8) From subsection (g) to the extent that this system is exempted from other provisions of the Privacy Act.

[Order No. 645-76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 6-86, 51 FR 10000, Apr. 24, 1986; Order No. 113-96, 61 FR 6316, Feb. 20, 1996; Order No. 114-96, 61 FR 6317, Feb. 20, 1996; Order No. 115-96, 61 FR 6319, Feb. 20, 1996; Order No. 279-2002, 67 FR 51754, Aug. 9, 2002; Order No. 280-2002, 67 FR 51755, Aug. 9, 2002; Order No. 281-2002, 67 FR 51756, Aug. 9, 2002; Order No. 004-2006, 71 FR 8805, Feb. 21, 2006]

§ 16.98 Exemption of the Drug Enforcement Administration (DEA)—limited access.

(a) The following systems of records are exempt from 5 U.S.C. 552a(c)(3) and (d):

(1) Automated Records and Consummated Orders System/Diversion Analysis and Detection System (ARCOS/DADS) (Justice/DEA-003)

(2) Controlled Substances Act Registration Records (Justice/DEA-005)

(3) Registration Status/Investigatory Records (Justice/DEA-012)

(b) These exemptions apply only to the extent that information in these systems is subject to exemption pursuant to 5 U.S.C. 552a(k)(2). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because release of the disclosure accounting would enable the subject of an investigation to gain valuable information concerning the nature and scope of the investigation and seriously hamper the regulatory functions of the DEA.

(2) From subsection (d) because access to records contained in these systems may provide the subject of an investigation information that could enable him to avoid compliance with the Drug Abuse Prevention and Control Act of 1970 (Pub. L. 91-513).

(c) Systems of records identified in paragraphs (c)(1) through (c)(7) below are exempted pursuant to the provisions of 5 U.S.C. 552a (j)(2) from subsections (c)(3) and (4); (d)(1), (2), and (4); (e)(1), (2) and (3), (e)(5), (e)(8); and (g) of 5 U.S.C. 552a. In addition, systems of records identified in paragraphs (c)(1), (c)(2), (c)(3), (c)(4), (c)(5), and (c)(6) below are also exempted pursuant to the provisions of 5 U.S.C. 552a (k)(1) from subsections (c)(3); (d)(3) and (4); and (e)(1):

(1) Air Intelligence Program (Justice/DEA-001)

(2) Clandestine Laboratory Seizure System (CLSS) (Justice/DEA-002)

(3) Investigative Reporting and Filing System (Justice/DEA-008)

(4) Planning and Inspection Division Records (Justice/DEA-010)

(5) Operation Files (Justice/DEA-011)

(6) Security Files (Justice/DEA-013)

(7) System to Retrieve Information from Drug Evidence (STRIDE/Ballistics) (Justice/DEA-014)

(d) Exemptions apply to the following systems of records only to the extent that information in the systems is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2):

Intelligence Program (Justice/DEA-001); Clandestine Laboratory Seizure System (CLSS) (Justice/DEA-002); Planning and Inspection Division Records (Justice/DEA-010); and S Files (Justice/DEA-013). Exemptions apply to the Investigative Reporting and Filing System (Justice/DEA-008) only to the extent that information in the system is subject to exempt pursuant to 5 U.S.C. 552a(j) (2) and (k)(1). Exemptions apply to the Operations Files (Justice/DEA-011) only to the extent that information in the system is subject to exempt pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). Exemptions apply to the System to Retrieve Information from Drug Evidence (STRIDE/Ballistics) (Justice/DEA-014) only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because release of disclosure accounting would provide to the subjects of an investigation significant information concerning the nature of the investigation and thus would present the same impediments to law enforcement as those enumerated in paragraph (d)(3) regarding exemption from subsection (d).

(2) From subsection (c)(4) to the extent that it is not applicable because an exemption is claimed from subsection (d).

(3) From the access provisions of subsection (d) because access to records in this system would present a serious impediment to law enforcement. Specifically, it could in the record subject of an actual or potential criminal, civil, or regulatory investigation of the existence of that investigation; of the nature and scope of the information and evidence obtained as to his activities; of the identity of confidential sources, witnesses, and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. Similarly, it may alert collateral suspects yet unprosecuted in closed cases and could prevent the successful completion of the investigation; endanger the life, health, or physical safety of confidential sources, witnesses, and law enforcement personnel, and to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony; or it may simply reveal a sensitive investigative technique. In addition, granting access to such information could result in the disclosure of confidential/security-sensitive or other information that would constitute an unwarranted invasion of the personal privacy of parties. Finally, access to the records could result in the release of properly classified information which would compromise the national defense or disrupt foreign policy. From the amendment provisions of subsection (d) because amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) because the application of this provision could impair investigation and interfere with the law enforcement responsibilities of the DEA for the following reasons:

(i) It is not possible to detect relevance or necessity of specific information in the early stages of a civil, criminal or other law enforcement investigation, case, or matter, including investigations during which DEA may obtain properly classified information. Relevance and necessity are questions of judgment and timing, and it is only after the information is evaluated that the relevance and necessity of such information can be established.

(ii) During the DEA's investigative activities DEA may detect the violation of either drug- or non-drug related laws. In the interests of effective law enforcement, it is necessary to retain all information obtained because it can aid in establishing patterns of activity and valuable leads for Federal and other law enforcement agencies or otherwise assist such agencies in discharging their law enforcement responsibilities. Such information may include properly classified information, the retention of which could be in the interests of national defense and/or foreign policy.

(5) From subsection (e)(2) because, in some instances, the application of this provision presents a serious impediment to law enforcement for the following reasons:

(i) The subject of an investigation would be placed on notice as to the existence of an investigation and would therefore be able to avoid detection or apprehension, to improperly influence witnesses, to destroy evidence, or to fabricate testimony.

(ii) In certain circumstances the subject of an investigation cannot be required to provide information to investigators, and information relating to a subject's illegal acts must be obtained from other sources.

(iii) In any investigation it is necessary to obtain evidence from a variety of sources other than the subject of the investigation in order to verify the evidence necessary for successful prosecution.

(6) From subsection (e)(3) because the requirements thereof would constitute a serious impediment to law enforcement in that they could compromise the existence of an actual or potential confidential investigation and/or permit the record subject to speculate on the existence of a potential confidential source, and endanger the life, health or physical safety or either

actual or potential confidential informants and witnesses, and of investigators/law enforcement personnel. In addition, the notification requirement of subsection (e)(3) could impede collection of that information from the record subject, making it necessary to collect the information from third party sources and thereby inhibiting law enforcement efforts.

(7) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of confidential intelligence necessary for effective law enforcement.

(8) From subsection (e)(8) because the application of this provision could prematurely reveal an ongoing criminal investigation to the subject of the investigation, and could reveal investigative techniques, procedures, or evidence.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d) pursuant to subsections (j)(2), (k)(1) and (k)(2) of the Privacy Act.

(e) The following systems of records are exempt from 5 U.S.C. 552a (d)(1) and (e)(1):

(1) Grants of Confidentiality Files (GCF) (Justice/DEA-017), and

(2) DEA Applicant Investigations (Justice/DEA-018).

(f) These exemptions apply only to the extent that information in these systems is subject to an exemption pursuant to 5 U.S.C. 552a(k)(5). Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (d)(1) because many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning an applicant for a grant of confidentiality with DEA. By permitting access to information which may reveal the identity of the source of that information—after a promise of confidentiality has been given—DEA would breach

promised confidentiality. Ultimately, such breaches would restrict the free flow of information which is vital to a determination of an applicant's qualifications for a grant.

(2) From subsection (e)(1) because in the collection of information for investigative and evaluation purposes, it is impossible to determine in advance what exact information may be of assistance in determining the qualifications and suitability of a candidate. Information which may appear irrelevant, when combined with other apparently irrelevant information, can on occasion provide a composite picture of an applicant which assists in determining whether a grant of confidentiality is warranted.

(g) The following system of records is exempt from 5 U.S.C. 552a (c)(3) and (4); (d)(1), and (4); (e)(1), (2), (3), (5), and (8); and (g): El Paso Intelligence Center (EPIC) Seizure (ESS) (JUSTICE/DEA-022). These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2). Where compliance would not appear to interfere with or adversely affect the law enforcement activities or counter-drug purposes of this system, and the overall law enforcement process, the application for exemption may be waived by the DEA in its sole discretion.

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting and disclosures from records concerning him/her would potentially reveal any investigative information in the individual. Revealing this information would permit the subject of an investigation to determine whether he is the subject of an investigation, or to obtain valuable information concerning the nature of that investigation and the information obtained, or the identity of witnesses and informants. Similarly, disclosure of this information could reasonably be expected to compromise ongoing investigatory efforts by notifying the record subject that he/she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(2) From subsection (c)(4) because this system is exempt from the access and amendment provisions of subsection (d).

(3) From subsections (d)(1), (2), (3), and (4) because these provisions concern individual access to and amendment of records contained in this system, which consists of counter-drug and criminal investigatory records. Compliance with these provisions could alert the sub

an investigation of an actual or potential criminal, civil, or regulatory violation of the exist that investigation, of the nature and scope of the information and evidence obtained as activities, of the identity of witnesses and informants, or would provide information that c enable the subject to avoid detection or apprehension. These factors would present a s impediment to effective law enforcement because they could prevent the successful completion of the investigation; endanger the physical safety of witnesses or informants lead to the improper influencing of witnesses, the destruction of evidence, or the fabrica testimony.

(4) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary to complete an identity comparison between the individual being screened and a known or suspected criminal or terrorist. Also, it may not always be known what information will be relevant to law enforcement for the purpose of conducting an operational response or on-going investigation.

(5) From subsection (e)(2) because application of this provision could present a serious impediment to law enforcement and counter-drug efforts in that it would put the subject investigation, study or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counter-drug investigations is such that vital information about an individual frequently can be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(6) From subsection (e)(3) because the requirements thereof would constitute a serious impediment to law enforcement in that they could compromise the existence of an actual or potential confidential investigation and/or permit the record subject to speculate on the existence of a potential confidential source, and endanger the life, health or physical safety of either actual or potential confidential informants and witnesses, and of investigators/law enforcement personnel. In addition, the notification requirement of subsection (e)(3) could impede collection of that information from the record subject, making it necessary to collect the information from third party sources and thereby inhibiting law enforcement efforts.

(7) From subsection (e)(5) because many of the records in this system are derived from domestic record systems and therefore it is not possible for the DEA and EPIC to vouch for their compliance with this provision. In addition, EPIC supports but does not conduct investigations; therefore, it must be able to collect information related to illegal drug and

criminal activities and encounters for distribution to law enforcement and intelligence agencies that do conduct counter-drug investigations. In the collection of information for law enforcement and counter-drug purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by (e)(5) would limit the ability of those agencies, trained investigators and intelligence analysts to exercise their judgment in conducting investigations and impede the development of intelligence necessary for effective law enforcement and counterterrorism efforts. EPIC has, however, implemented internal quality assurance procedures to ensure that ESS data is as thorough, accurate, and current as possible. ESS is also exempt from the requirements of subsection (e)(5) in order to prevent the use of a challenge under subsection (e)(5) as a collateral means to obtain access to records in the ESS. ESS records are exempt from the access and amendment requirements of subsection (d) of the Privacy Act in order to protect the integrity of investigations. Exempting ESS from subsection (e)(5) serves to prevent the assertion of challenges to a record's accuracy, timeliness, completeness, and/or relevance under subsection (e)(5) to circumvent the exemption claimed from subsection (d).

(8) From subsection (e)(8) because to require individual notice of disclosure of information to compulsory legal process would pose an impossible administrative burden on the DE and EPIC and could alert the subjects of counter-drug, counterterrorism, law enforcement, and intelligence investigations to the fact of those investigations when not previously known. Additionally, compliance could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.

(9) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

[Order No. 88-94, 59 FR 29717, June 9, 1994, as amended by Order No. 127-97, 62 FR 10000, Jan. 21, 1997; Order No. 009-2003, 68 FR 14140, Mar. 24, 2003; 72 FR 54825, Sept. 27, 2007]

§ 16.99 Exemption of the Immigration and Naturalization Service Systems-limited access

(a) The following systems of records of the Immigration and Naturalization Service are exempt from 5 U.S.C. 552a (c) (3) and (4), (d), (e) (1), (2) and (3), (e) (4)(G) and (H), (e) (5) and (g):

(1) The Immigration and Naturalization Service Alien File (A-File) and Central Index System (CIS), JUSTICE/INS-001A.

(2) The Immigration and Naturalization Service Index System, JUSTICE/INS-001 which consists of the following subsystems:

(i) Agency Information Control Record Index.

(ii) Alien Enemy Index.

(iii) Congressional Mail Unit Index.

(iv) Air Detail Office Index.

(v) Anti-smuggling Index (general).

(vi) Anti-smuggling Information Centers Systems for Canadian and Mexican Borders.

(vii) Border Patrol Sectors General Index System.

(viii) Contact Index.

(ix) Criminal, Narcotic, Racketeer and Subversive Indexes.

(x) Enforcement Correspondence Control Index System.

(xi) Document Vendors and Alterers Index.

(xii) Informant Index.

(xiii) Suspect Third Party Index.

(xiv) Examination Correspondence Control Index.

(xv) Extension Training Enrollee Index.

(xvi) Intelligence Index.

(xvii) Naturalization and Citizenship Indexes.

(xviii) Personnel Investigations Unit Indexes.

(xix) Service Look-Out Subsystem.

(xx) White House and Attorney General Correspondence Control Index.

(xxi) Fraudulent Document Center Index.

(xxii) Emergency Reassignment Index.

(xxiii) Alien Documentation, Identification, and Telecommunication (ADIT) System.

The exemptions apply to the extent that information in these subsystems is subject to exemption pursuant to 5 U.S.C. 552a (j)(2) and (k)(2).

(3) The Immigration and Naturalization Service "National Automated Immigration Lookout System (NAIS) JUSTICE/INS-032." The exemptions apply only to the extent that records in the system are subject to exemptions pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting for disclosure pursuant to the routine uses published for these subsystems would permit the subject of a criminal or civil investigation to obtain valuable information concerning the nature of that investigation and present a serious impediment to law enforcement.

(2) From subsection (c)(4) since an exemption is being claimed for subsection (d), this subsection will not be applicable.

(3) From subsection (d) because access to the records contained in these subsystems would inform the subject of a criminal or civil investigation of the existence of that investigation

provide the subject of the investigation with information that might enable him to avoid detection or apprehension, and present a serious impediment to law enforcement.

(4) From subsection (e)(1) because in the course of criminal or civil investigations, the Immigration and Naturalization Service often obtains information concerning the violation of laws other than those relating to violations over which INS has investigative jurisdiction. In the interests of effective law enforcement, it is necessary that INS retain this information since it can aid in establishing patterns of criminal activity and provide valuable leads for those law enforcement agencies that are charged with enforcing other segments of the criminal law.

(5) From subsection (e)(2) because in a criminal or civil investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection or apprehension.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the physical safety of confidential informants.

(7) From subsections (e)(4) (G) and (H) because these subsystems of records are exempt from individual access pursuant to subsection (j) of the Privacy Act of 1974.

(8) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(9) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the Immigration and Naturalization Service's ability to issue administrative subpoenas and c

reveal investigative techniques and procedures.

(10) From subsection (g) because these subsystems of records are compiled for law enforcement purposes and have been exempted from the access provisions of subsection (f).

(11) In addition, these systems of records are exempt from subsections (c)(3), (d), (e)(1), (G) and (H) to the extent they are subject to exemption pursuant to 5 U.S.C. 552a(k)(1). permit access to records classified pursuant to Executive Order would violate the Executive Order protecting classified information.

(c) The Border Patrol Academy Index Subsystem is exempt from 5 U.S.C. 552a (d) and

This exemption applies only to the extent that information in this subsystem is subject to exemption pursuant to 5 U.S.C. 552a(k).

(d) Exemptions for the particular subsections are justified for the following reasons.

(1) From subsection (d) because exemption is claimed only for those testing and examination materials used to determine an individual's qualifications for retention and promotion in Immigration and Naturalization Service. This is necessary to protect the integrity of testing materials and to insure fair and uniform examinations.

(2) From subsection (f) because the subsystem of records has been exempted from the provisions of subsection (d).

(e) The Orphan Petitioner Index and Files (Justice/INS-007) system of records is exempt from 5 U.S.C. 552a(d). This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(1).

(f) Exemption from paragraph (d) of this section is claimed solely because of the possible receipt of classified information during the course of INS investigation of prospective adoptive parents.

Although it would be rare, prospective adoptive parents may originally be from foreign countries (for example) and information received on them from their native countries may

require classification under Executive Order 12356 which safeguards national security information. If such information is relevant to the INS determination with respect to adp the information would be kept in the file and would be classified accordingly. Therefore, could not be granted to the record subject under the Privacy Act without violating E.O.

(g) The Office of Internal Audit Investigations Index and Records (Justice/INS-002) syst records is exempt under the provisions of 5 U.S.C. 552a(j)(2) from subsections (c)(3) an (d); (e)(1), (2), (3), (5) and (8); and (g), but only to the extent that this system contains r within the scope of subsection (j)(2), and to the extent that records in the system are su exemption therefrom. In addition, this system of records is also exempt under the provis 5 U.S.C. 552a(k)(2) from subsections (c)(3); (d); and (e)(1), but only to the extent that th system contains records within the scope of subsection (k)(2), and to the extent that rec the system are subject to exemption therefrom.

(h) The following justification apply to the exemptions from particular subsections:

(1) From subsection (c)(3) because the release of the disclosure accounting for disclos could permit the subject of an actual or potential criminal or civil investigation to obtain v information concerning the existence and nature of the investigation, the fact that individ are subjects of the investigation, and present a serious impediment to law enforcement.

(2) From subsection (c)(4) to the extent that the exemption from subsection (d) is applic Subsection (c)(4) will not be applicable to the extent that records in the system are prop withholdable under subsection (d).

(3) From the access and amendment provisions of subsection (d) because access to th records contained in this system of records could inform the subject of a criminal or civil investigation of the existence of that investigation; of the nature and scope of the inform and evidence obtained as to their activities; of the identity of confidential sources, witnes and law enforcement personnel; and of information that may enable the subject to avoid detection or apprehension. Such disclosures would present a serious impediment to eff law enforcement where they prevent the successful completion of the investigation; end the physical safety of confidential sources, witnesses, and law enforcement personnel; lead to the improper influencing of witnesses, the destruction of evidence, or the fabrica testimony. In addition, granting access to these records could result in a disclosure that constitute an unwarranted invasion of the privacy of third parties. Amendment of the rec would interfere with ongoing investigations and law enforcement activities and impose a

impossible administrative burden by requiring investigations to be continuously reinvest

(4) From subsection (e)(1) because in the course of criminal or civil investigations, the Immigration and Naturalization Service often obtains information concerning the violation laws other than those relating to violations over which INS has investigative jurisdiction, interests of effective law enforcement, it is necessary that INS retain this information since it can aid in establishing patterns of criminal activity and provide valuable leads for those enforcement agencies that are charged with enforcing other segments of the criminal la

(5) From subsection (e)(2) because in a criminal investigation, the requirement that information be collected to the greatest extent possible from the subject individual would present an impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection and apprehension.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to criminal law enforcement in that it could compromise the existence of a confidential investigation, reveal the identity of confidential sources of information and endanger the life or physical safety of confidential informants.

(7) From subsection (e)(5) because in the collection of information for criminal law enforcement purposes it is impossible to determine in advance what information is accurate, relevant and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(8) From subsection (e)(8) because the individual notice requirements of subsection (e)(8) could present a serious impediment to criminal law enforcement as this could interfere with the Immigration and Naturalization Service's ability to issue administrative subpoenas and could reveal investigative techniques and procedures.

(9) From subsection (g) for those portions of this system of records that were compiled for criminal law enforcement purposes and which are subject to exemption from the access

provisions of subsections (d) pursuant to subsection (j)(2).

(i) The Law Enforcement Support Center Database (LESC) (Justice/INS-023) system of records is exempt under the provisions of 5 U.S.C. 552a(j)(2) from subsections (c) (3) and (d); (e) (1), (2), (3), (5), (8) and (g); but only to the extent that this system contains records within the scope of subsection (j)(2), and to the extent that records in the system are subject to exemption therefrom. In addition, this system of records is also exempt in part under the provisions of 5 U.S.C. 552a(k)(2) from subsections (c)(3); (d); and (e)(1), but only to the extent that this system contains records within the scope of subsection (k)(2), and to the extent records in the system are subject to exemption therefrom.

(j) The following justifications apply to the exemptions from particular subsections:

(1) From subsection (c)(3) for reasons stated in paragraph (h)(1) of this section.

(2) From subsection (c)(4) for reasons stated in paragraph (h)(2) of this section.

(3) From the access and amendment provisions of subsection (d) because access to the records contained in this system of records could inform the subject of a criminal or civil investigation of the existence of that investigation; of the nature and scope of the information and evidence obtained as to their activities; and of information that may enable the subject to avoid detection or apprehension. Such disclosures would present a serious impediment to effective law enforcement where they prevent the successful completion of the investigation or other law enforcement operation such as deportation or exclusion. In addition, granting access to these records could result in a disclosure that would constitute an unwarranted invasion of the privacy of third parties. Amendment of the records would interfere with ongoing investigations and law enforcement activities and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(4) From subsection (e)(1) for reasons stated in paragraph (h)(4) of this section.

(5) From subsection (e)(2) for reasons stated in paragraph (h)(5) of this section.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to criminal law enforcement in that it could compromise the existence of a

confidential investigation.

(7) From subsection (e)(5) for reasons stated in paragraph (h)(7) of this section.

(8) From subsection (e)(8) for reasons stated in paragraph (h)(8) of this section.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d).

(k) The Attorney/Representative Complaint/Petition File (JUSTICE/INS-022) system of records is exempt under the provisions of 5 U.S.C. 552a (j)(2) from subsections (c)(3) and (4); (e)(1), (2), (3), (5), and (8); and (g); but only to the extent that this system contains records within the scope of subsection (j)(2), and to the extent that records in this system are subject to exemption therefrom. In addition, this system of records is also exempt in part under the provisions of 5 U.S.C. 552a (k)(2) from subsections (c)(3); (d); and (e)(1), but only to the extent that this system contains records within the scope of subsection (k)(2), and to the extent that records in this system are subject to exemption therefrom.

(l) The following justifications apply to the exemptions from particular subsections:

(1) From subsection (c)(3) for reasons stated in paragraph (h)(1) of this section.

(2) From subsection (c)(4) for reasons stated in paragraph (h)(2) of this section.

(3) From the access and amendment provisions of subsection (d) for reasons stated in paragraph (h)(3) of this section.

(4) From subsection (e)(1) for reasons stated in paragraph (h)(4) of this section.

(5) From subsection (e)(2) for reasons stated in paragraph (h)(5) of this section.

(6) From subsection (e)(3) for reasons stated in paragraph (h)(6) of this section.

(7) From subsection (e)(5) for reasons stated in paragraph (h)(7) of this section.

(8) From subsection (e)(8) for reasons stated in paragraph (h)(8) of this section.

(9) From subsection (g) to the extent that the system is exempt from the access and amendment provisions of subsection (d).

(m) The Worksite Enforcement Activity and Records Index (LYNX) (JUSTICE/INS-025) system of records is exempt under the provisions of 5 U.S.C. 552a (j)(2) from subsections (c)(3); (4); (d); (e)(1), (2), (3), (5), and (8); and (g); but only to the extent that this system contains records within the scope of subsection (j)(2), and to the extent that records in this system are subject to exemption therefrom. In addition, this system of records is also exempt in part under the provisions of 5 U.S.C. 552a(k)(2) from subsections (c)(3); (d); and (e)(1), but only to the extent that this system contains records within the scope of subsection (k)(2), and to the extent that records in this system are subject to exemption therefrom.

(n) The following justifications apply to the exemptions from particular subsections:

(1) From subsection (c)(3) for reasons stated in paragraph (h)(1) of this section.

(2) From subsection (c)(4) for reasons stated in paragraph (h)(2) of this section.

(3) From the access and amendment provisions of subsection (d) for reasons stated in paragraph (h)(3) of this section.

(4) From subsection (e)(1) for reasons stated in paragraph (h)(4) of this section.

(5) From subsection (e)(2) for reasons stated in paragraph (h)(5) of this section.

(6) From subsection (e)(3) for reasons stated in paragraph (h)(6) of this section.

(7) From subsection (e)(5) for reasons stated in paragraph (h)(7) of this section.

(8) From subsection (e)(8) for reasons stated in paragraph (h)(8) of this section.

(9) From subsection (g) to the extent that the system is exempt from the access and amendment provisions of subsection (d).

[Order No. 645-76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 688-77, 42

10001, Feb. 18, 1977; Order No. 6–84, 49 FR 20812, May 17, 1984; Order No. 25–88, 54 FR 41161, Oct. 20, 1988; Order No. 137–97, 62 FR 34169, June 25, 1997; Order No. 142–97, 62 FR 44083, Aug. 19, 1997; Order No. 196–2000, 65 FR 21139, Apr. 20, 2000; Order No. 197–2000, 65 FR 21140, Apr. 20, 2000]

§ 16.100 Exemption of Office of Justice Programs—limited access.

(a) The following system of records is exempt from 5 U.S.C. 552a(d):

(1) The Civil Rights Investigative System (JUSTICE/OJP–008).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

(b) Exemption from subsection (d) is claimed since access to information in the Civil Rights Investigative System prior to final administrative resolution will deter conciliation and compliance efforts. Consistent with the legislative purpose of the Privacy Act of 1974, disclosure of information from the system will be made on a case-by-case basis and information will be made available where it does not compromise the complaint and compliance process. In addition, where explicit promises of confidentiality must be made to a source during an investigation, disclosure will be limited to the extent that the identity of such confidential sources will not be compromised.

[Order No. 645–76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 5–78, 43 FR 15448, Aug. 17, 1978; Order No. 43–80, 45 FR 6780, Jan. 30, 1980; Order No. 6–86, 51 FR 15448, Apr. 24, 1986; Order NO. 6–236–2001, 66 FR 35374, July 5, 2001]

§ 16.101 Exemption of U.S. Marshals Service Systems—limited access, as indicated

(a) The following system of records is exempt from 5 U.S.C. 552(a)(c) (3) and (4), (d), (e)(2) and (3), (e)(4) (G) and (H), (e)(5), (e)(8), (f) and (g):

(1) Warrant Information System (JUSTICE/USM–007).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of disclosure accounting for disclosure pursuant to subsection (b) of the Act, including those permitted under routine uses published for this system of records would permit a person to determine whether he is the subject of a criminal investigation, and to determine whether a warrant has been issued against him, would therefore present a serious impediment to law enforcement.

(2) From subsection (c)(4) since an exemption is being claimed for subsection (d) of this section is inapplicable.

(3) From subsection (d) because access to records would inform a person for whom a warrant has been issued of the nature and scope of information obtained as to his activities, the identity of informants, and afford the person sufficient information to enable the subject to avoid apprehension. These factors would present a serious impediment to law enforcement that they would thwart the warrant process and endanger lives of informants etc.

(4) From subsections (e)(1) and (e)(5) because the requirements of these subsections would present a serious impediment to law enforcement in that it is impossible to determine in advance what information collected during an investigation will be important or crucial to the apprehension of Federal fugitives. In the interest of effective law enforcement, it is appropriate in a thorough investigation to retain seemingly irrelevant, untimely, or inaccurate information which, with the passage of time, would aid in establishing patterns of activity and provide investigative leads toward fugitive apprehension and assist in law enforcement activities of other agencies.

(5) From subsection (e)(2) because the requirement that information be collected to the greatest extent practical from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the warrant and would therefore be able to avoid detection or apprehension.

(6) From subsection (e)(3) because the requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal identity of confidential informants.

(7) From subsections (e)(4) (G) and (H) since an exemption is being claimed for subsection (d) of the Act, these subsections are inapplicable.

(8) From subsection (e)(8) because the individual notice requirement of this subsection present a serious impediment to law enforcement in that it would give persons sufficient warning to avoid warrants, subpoena, etc.

(9) From subsection (f) because procedures for notice to an individual pursuant to subsection (f)(1) as to existence of records pertaining to him dealing with warrants must be exempt because such notice to individuals would be detrimental to the successful service of a warrant. Since an exemption is being claimed for subsection (d) of the Act the rules required pursuant to subsections (f) (2) through (5) are inapplicable to this system of records.

(10) From subsection (g) since an exemption is being claimed for subsection (d) and (f) section is inapplicable and is exempted for the reasons set forth for these subsections.

(c) The following system of records is exempt from 5 U.S.C. 552a (c) (3) and (4), (d), (e) and (3), (e)(4) (G) and (H), (e)(8), (f)(2) and (g):

(1) Witness Security System (JUSTICE/USM-008).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of the disclosure accounting for disclosure made pursuant to subsection (b) of the Act including those permitted under routine use published for this system of records would hamper the effective functioning of the Witness Security Program which by its very nature requires strict confidentiality vis-a-vis the records.

(2) From subsection (c)(4) for the reason stated in (b)(2) of this section.

(3) From subsection (d) because the U.S. Marshals Service Witness Security Program and efforts of law enforcement officials to prevent, control or reduce crime. Access to records

present a serious impediment to effective law enforcement through revelation of confidential sources and through disclosure of operating procedures of the program, and through increased exposure of the program to the public.

(4) From subsection (e)(2) because in the Witness Security Program the requirement that information be collected to the greatest extent possible from the subject individual would constitute an impediment to the program, which is sometimes dependent on sources other than the subject witness for verification of information pertaining to the witness.

(5) From subsection (e)(3) for the reason stated in (b)(6) of this section.

(6) From subsection (e)(4) (G) and (H) for the reason stated in (b)(7) of this section.

(7) From subsection (e)(8) for the reason stated in (b)(8) of this section.

(8) From subsection (f)(2) since an exemption is being claimed for subsection (d) of the rules required pursuant to subsection (f) (2) through (5) are inapplicable to this system records.

(9) From subsection (g) for the reason stated in (b)(10) of this section.

(e) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(1) and (3), (e)(4)(G) and (H), (e)(5), (e)(8), (f) and (g).

(1) Internal Affairs System (JUSTICE/USM-002)—Limited access. These exemptions apply to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2), (k)(2) or (k)(5). Where compliance would not interfere with or adversely affect law enforcement process, the USMS may waive the exemptions, either partially or totally.

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsections (c)(3) and (d) to the extent that release of the disclosure accounting information would impede or interfere with civil or criminal law enforcement efforts, reveal a source who furnished information to the Government in confidence, and/or result in an unwarranted invasion of the personal privacy of collateral record subjects or other third party individuals.

(2) From subsection (c)(4) for the reason stated in (b)(2) of this section.

(3) From subsection (e)(1) to the extent that it is necessary to retain all information in or to impede, compromise, or interfere with civil or criminal law enforcement efforts, e.g., where the significance of the information may not be readily determined and/or where such information may provide leads or assistance to Federal and other law agencies in discharging their law enforcement responsibilities.

(4) From subsection (e)(2) because the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to compromise the investigation and avoid detection or apprehension.

(5) From subsection (e)(3) for the reason stated in (b)(6) of this section.

(6) From subsections (e)(4) (G) and (H) for the reason stated in (b)(7) of this section.

(7) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can only be determined by a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability to collect information for law enforcement purposes and interfere with the preparation of a complete investigative report or otherwise impede effective law enforcement.

(8) From subsection (e)(8) because the individual notice requirement of this subsection would present a serious impediment to law enforcement in that the subject of the investigation would be alerted as to the existence of the investigation and therefore be able to compromise the investigation and avoid detection, subpoena, etc.

(9) From subsection (f) because procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records dealing with investigations of criminal or civil law violations would enable the individual to compromise the investigation and evade detection or apprehension. Since an exemption is being claimed for subsection (d) of the Act, the rules required pursuant to subsections (f)(2) through (f)(5) are not applicable to this system.

(10) From subsection (g) for the reason stated in (b)(10) of this section.

(g) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) and (3), (e)(4) (G) and (H), (e)(5), (e)(8), (f) and (g):

(1) U.S. Marshals Service Threat Analysis Information System (JUSTICE/USM-009).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to release the disclosure accounting would permit a to determine whether he or she has been identified as a specific threat to USMS protect and to determine the need for countermeasures to USMS protective activities and there present a serious impediment to law enforcement.

(2) From subsection (c)(4) because it is inapplicable since an exemption is being claimed subsection (d).

(3) From subsection (d) because to permit access to records would inform a person of the nature and scope of information obtained as to his or her threat-related activities and of identity of confidential sources, and afford the person sufficient information to develop countermeasures to thwart protective arrangements and endanger lives of USMS protect informants, etc. To permit amendment of the records would interfere with ongoing criminal enforcement and impose an impossible administrative burden requiring criminal investigation to be continuously reinvestigated.

(4) From subsections (e) (1) and (5) because the collection of investigatory information to assess the existence, extent and likelihood of a threat situation necessarily includes material from which it is impossible to identify and segregate information which may not be impede the conduct of a thorough assessment. It is often impossible to determine in advance if information collected is accurate, relevant, timely and complete but, in the interests of developing effective protective measures, it is necessary that the U.S. Marshals Service release this information in order to establish patterns of activity to aid in accurately assessing the situations. The restrictions of subsections (e) (1) and (5) would impede the protective

responsibilities of the Service and could result in death or serious injury to Marshals Service protectees.

(5) From subsection (e)(2) because to collect information from the subject individual would serve notice that he or she is identified as a specific threat to USMS protectees and would enable the subject individual to develop countermeasures to protective activities and thereby present a serious impediment to law enforcement.

(6) From subsection (e)(3) because to inform individuals as required by this subsection would enable the subject individual to develop countermeasures to USMS protective arrangements, identify confidential sources and thereby present a serious impediment to law enforcement.

(7) From subsections (e)(4) (G) and (H) because they are inapplicable since an exemption is being claimed for subsections (d) and (f) of the Act.

(8) From subsection (e)(8) because to serve notice would give persons sufficient warning to develop countermeasures to protective arrangements and thereby present a serious impediment to law enforcement through compromise of protective procedures, etc.

(9) From subsection (f) because this system of records is exempt from the provisions of subsection (d).

(10) From subsection (g) because it is inapplicable since an exemption is being claimed under subsections (d) and (f).

(i) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (d):

(1) Judicial Facility Security Index System (JUSTICE/USM-010)

These exemptions apply only to the extent that information in this system is exempt pursuant to 5 U.S.C. 552a(k)(5).

(j) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) only to the extent that release of the disclosure accounting would reveal the identity of a confidential source.

(2) From subsection (d) only to the extent that access to information would reveal the identity of a confidential source.

(k) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1) and (3), (e)(4) (G) and (H), (e)(5), (e)(8), (f) and (g):

(1) U.S. Marshals Service Freedom of Information/Privacy Act (FOIA/PA) Files (JUSTICE/USM-012).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(2) and (k)(5).

(l) Because this system contains Department of Justice civil and criminal law enforcement investigatory records, exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to release the disclosure accounting would permit the subject of an investigation to obtain valuable information concerning the existence and nature of the investigation and present a serious impediment to law enforcement.

(2) From subsection (c)(4) because that portion of this system which consists of investigatory records compiled for law enforcement purposes is being exempted from the provisions of subsection (d), rendering this provision not applicable.

(3) From subsection (d) because to permit access to investigatory records would reveal identity of confidential sources and impede ongoing investigative or law enforcement activities by the premature disclosure of information related to those efforts. To permit amendment of records would interfere with ongoing criminal law enforcement and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(4) From subsections (e) (1) and (5) because it is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete. In the interests of effective law enforcement, it is necessary to retain this information to establish patterns of activity and provide leads in criminal investigations.

(5) From subsection (e)(2) because to collect information from the subject individual would

serve notice that he or she is the subject of criminal investigative or law enforcement action and thereby present a serious impediment to law enforcement.

(6) From subsection (e)(3) because to inform individuals as required by this subsection enable the subject individual to identify confidential sources, reveal the existence of an investigation, and compromise law enforcement efforts.

(7) From subsections (e)(4) (G) and (H) because they are inapplicable since an exemption is being claimed for subsections (d) and (f) for investigatory records contained in this system.

(8) From subsection (e)(8) because to serve notice would give persons sufficient warning to evade law enforcement efforts.

(9) From subsection (f) because investigatory records contained in this system are exempt from the provisions of subsection (d).

(10) From subsection (g) because it is inapplicable since an exemption is being claimed for subsections (d) and (f).

(m) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e)(1) and (3), (e)(4) (G) and (H), (e)(8), (f) and (g):

(1) U.S. Marshals Service Administrative Proceedings, Claims and Civil Litigation Files (JUSTICE/USM-013).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) or (k)(5).

(n) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to release the disclosure accounting for disclosures pursuant to the routine uses published for this system would permit the subject of a criminal case or matter under investigation, or a case or matter in litigation, or under regulatory administrative review or action, to obtain valuable information concerning the nature of the investigation, case or matter, and present a serious impediment to law enforcement or criminal legal activities, or reveal a confidential source.

(2) From subsection (c)(4) because the exemption claimed for subsection (d) will make section inapplicable.

(3) From subsection (d) because to permit access to records contained in this system would provide information concerning litigation strategy, or case development, and/or reveal the nature of the criminal or civil case or matter under investigation or administrative review, litigation, and present a serious impediment to law enforcement or civil legal activities, or a confidential source.

(4) From subsection (e)(2) because effective legal representation, defense, or claim adjudication necessitates collecting information from all individuals having knowledge of criminal or civil case or matter. To collect information primarily from the subject individuals present a serious impediment to law enforcement or civil legal activities.

(5) From subsection (e)(3) because to inform the individuals as required by this subsection would permit the subject of a criminal or civil matter under investigation or administrative review to compromise that investigation or administrative review and thereby impede law enforcement efforts or civil legal activities.

(6) From subsections (e)(4) (G) and (H) because these provisions are inapplicable since system is exempt from subsections (d) and (f) of the Act.

(7) From subsection (e)(8) because to serve notice would give persons sufficient warning to compromise a criminal or civil investigation or administrative review and thereby impede enforcement of civil legal activities.

(8) From subsection (f) because this system of records is exempt from the provisions of subsection (d).

(9) From subsection (g) because it is inapplicable since an exemption is claimed for subsections (d) and (f).

(o) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) (5) and (g):

(1) U.S. Marshals Service Prisoner Transportation System (JUSTICE/USM-003).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(p) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) where the release of the disclosure accounting for disclosure pursuant to subsection (b) of the Act would reveal a source who furnished information to the Government in confidence.

(2) From subsection (c)(4) to the extent that the system is exempt from subsection (d).

(3) From subsection (d) because access to records would reveal the names and other information pertaining to prisoners, including sensitive security information such as the identities and locations of confidential sources, e.g., informants and protected witnesses; disclose access codes, data entry codes and message routing symbols used in law enforcement communications systems to schedule and effect prisoner movements. Thus, a compromise of law enforcement communications systems would subject law enforcement personnel and other prisoners to harassment and possible danger, and present a serious threat to law enforcement activities. To permit amendment of the records would interfere with ongoing criminal law enforcement and impose an impossible administrative burden by requiring that information affecting the prisoner's security classification be continuously reinvestigated when contested by the prisoner, or by anyone on his behalf.

(4) From subsections (e) (1) and (5) because the security classification of prisoners is based upon information collected during official criminal investigations; and, in the interest of safe and secure prisoner movements it may be necessary to retain information the relevance, necessity, accuracy, timeliness, and completeness of which cannot be readily established, which may subsequently prove useful in establishing patterns of criminal activity or avoid them, and thus be essential to assigning an appropriate security classification to the prisoner. The restrictions of subsection (e) (1) and (5) would impede the information collection responsibilities of the USMS, and the lack of all available information could result in death or serious injury to USMS and other law enforcement personnel, prisoners in custody, and members of the public.

(5) From subsection (e)(2) because the requirement to collect information from the subject individual would impede the information collection responsibilities of the USMS in that the USMS is often dependent upon sources other than the subject individual for verification of information.

information pertaining to security risks posed by the individual prisoner.

(6) From subsection (g) to the extent that the system is exempt from subsection (d).

(q) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(3), (e)(5) and (e)(8) and (g):

(1) U.S. Marshals Service Prisoner Processing and Population Management System (JUSTICE/USM-005).

These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2).

(r) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to release the disclosure accounting would permit the subject of a criminal proceeding to determine the extent or nature of law enforcement authorities' knowledge regarding his/her alleged misconduct or criminal activities. The disclosure of such information could alert the subject to devise ways in which to conceal his/her activities and/or prevent law enforcement from learning additional information about his/her activities, or otherwise inhibit law enforcement efforts. In addition, where the individual is the subject of an ongoing or potential inquiry/investigation, such release could reveal the nature thereof prematurely, and may also enable the subject to determine the identity of witnesses and informants. Such disclosure could compromise the ongoing or potential inquiry/investigation, endanger the lives of witnesses and informants, or otherwise impede law enforcement efforts.

(2) From subsection (c)(4) to the extent that the system is exempt from subsection (d).

(3) From subsection (d) because to permit unlimited access would permit the subject of a criminal proceeding to determine the extent or nature of law enforcement authorities' knowledge regarding his/her alleged misconduct or criminal activities. The disclosure of information could alert the subject to devise ways in which to conceal his/her activities and prevent law enforcement from learning additional information about his/her activities, or otherwise inhibit law enforcement efforts. Disclosure would also allow the subject to obtain sensitive information concerning the existence and nature of security measures and jeopardize

the safe and secure transfer of the prisoner, the safety and security of other prisoners, informants and witnesses, law enforcement personnel, and the public. In addition, disclosure may enable the subject to learn prematurely of an ongoing or potential inquiry/investigation and may also permit him/her to determine the identities of confidential sources, informal protected witnesses. Such disclosure could compromise the ongoing or potential inquiry/investigation, endanger the lives of witnesses and informants, or otherwise impede or thwart law enforcement efforts. Disclosure may also constitute an unwarranted invasion of the personal privacy of third parties. Further, disclosure would reveal access codes, data entry codes and message routing symbols used in law enforcement communications systems. Access to such codes and symbols would permit the subject to impede the flow of law enforcement communications and compromise the integrity of law enforcement information and thus present a serious threat to law enforcement activities. To permit amendment of records would expose security matters, and would impose an impossible administrative burden by requiring that security precautions, and information pertaining thereto, be continuously reevaluated if contested by the prisoner, or by anyone on his or her behalf. Similarly, to require amendment could interfere with ongoing or potential inquiries/investigations by requiring such inquiries/investigations be continuously reinvestigated, or that information collected (regardless of its relevance and accuracy of which cannot readily be determined) be subjected to continuous change.

(4) From subsections (e)(1) and (5) because the system may contain investigatory information or information which is derived from information collected during official criminal investigations. In the interest of effective law enforcement and litigation, of securing the prisoner and of protecting the public, it may be necessary to retain information the relevance, necessity, accuracy, timeliness and completeness of which cannot be readily established. Such information may nevertheless provide investigative leads to other Federal or law enforcement agencies, or prove necessary to establish patterns of criminal activity or behavior, and/or be essential to the safe and secure detention (and movement) of prisoners. Further, the proposed amendment of (e)(1) and (e)(5) would restrict the ability of the USMS in exercising its judgment in retaining information during investigations or during the development of appropriate security measures and thus present a serious impediment to law enforcement efforts.

(5) From subsection (e)(2) because the requirement to collect information from the subject individual would impede the information collection responsibilities of the USMS which is dependent upon sources other than the subject individual for verification of information pertaining to security risks posed by the individual prisoner, to alleged misconduct or criminal activity of the prisoner, or to any matter affecting the safekeeping and disposition of the

individual prisoner.

(6) From subsection (e)(3) because to inform individuals as required by this subsection impede the information gathering process, reveal the existence of an ongoing or potential inquiry/investigation or security procedure, and compromise law enforcement efforts.

(7) From subsection (e)(8) because to serve notice would give persons sufficient warning to compromise an ongoing or potential inquiry/investigation and thereby evade and impede law enforcement and security efforts.

(8) From subsection (g) to the extent that the system is exempt from subsection (d).

(s) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) (3), (e) (5) and (e) (8) and (g):

Joint Automated Booking Stations, Justice/USM-014

(t) These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Where compliance would not interfere with or adversely affect the law enforcement process, the USMS may waive the exemptions, either partially or totally. Exemption from the particular subsections are justified for the following reasons:

(1) From subsections (c)(3) and (d) to the extent that access to records in this system or records may impede or interfere with law enforcement efforts, result in the disclosure of information that would constitute an unwarranted invasion of the personal privacy of a record subject or other third parties, and/or jeopardize the health and/or safety of third parties.

(2) Where access to certain records may be appropriate, exemption from the amendment provisions of subsection (d)(2) is necessary to the extent that the necessary and appropriate justification, together with proof of record inaccuracy, is not provided, and/or to the extent that numerous, frivolous requests to amend could impose an impossible administrative burden requiring agencies to continuously review booking and arrest data, much of which is collected from the arrestee during the arrest.

(3) From subsection (e)(1) to the extent that it is necessary to retain all information in or

to impede, compromise, or interfere with law enforcement efforts, e.g., where the significance of the information may not be readily determined and/or where such information may provide leads or assistance to Federal and other law enforcement agencies in discharging their enforcement responsibilities.

(4) From subsection (e)(2) because, in some instances, the application of this provision presents a serious impediment to law enforcement since it may be necessary to obtain and verify information from a variety of sources other than the record subject to ensure safekeeping, security, and effective law enforcement. For example, it may be necessary for medical and psychiatric personnel to provide information regarding the subject's behavior, physical health, or mental stability, etc. To ensure proper care while in custody, or it may be necessary to obtain information from a case agent or the court to ensure proper disposition of the subject individual.

(5) From subsection (e)(3) because the requirement that agencies inform each individual that it asks to supply information of such information as is required by subsection (e)(3) may, in some cases, impede the information gathering process or otherwise interfere with or compromise law enforcement efforts, e.g., the subject may deliberately withhold information or give erroneous information.

(6) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can only be determined by a court of law. The restrictions imposed by subsection (e)(5) would restrict the ability to collect information for law enforcement purposes and may prevent the eventual development of necessary criminal intelligence or otherwise impede effective law enforcement.

(7) From subsection (e)(8) to the extent that such notice may impede, interfere with, or otherwise compromise law enforcement and security efforts.

(8) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d).

(u) Consistent with the legislative purpose of the Privacy Act of 1974, the United States Marshals Service will grant access to nonexempt material in records which are maintained by the Service. Disclosure will be governed by the Department's Privacy Regulations, but v

limited to the extent that the identity of confidential sources will not be compromised; subject of an investigation of an actual or potential criminal, civil or regulatory violation will not be alerted to the investigation; the physical safety of witnesses, informants and law enforcement personnel will not be endangered; the privacy of third parties will not be violated; and the disclosure would not otherwise impede effective law enforcement. Whenever possible, information of the above nature will be deleted from the requested documents and the information made available. The controlling principle behind this limited access is to allow disclosure except those indicated above. The decisions to release information from these systems are made on a case-by-case basis.

[Order No. 645–76, 41 FR 12640, Mar. 26, 1976, as amended by Order No. 8–83, 48 FR 10000, Apr. 27, 1983; Order No. 10–86, 51 FR 20275, June 4, 1986; Order No. 11–86, 51 FR 20275, June 4, 1986; Order No. 61–92, 57 FR 3284, Jan. 29, 1992; Order No. 66–92, 57 FR 20275, May 14, 1992; Order No. 105–95, 60 FR 30467, June 9, 1995; Order No. 212–2001, 66 FR 6470, Jan. 22, 2001]

§ 16.102 Exemption of Drug Enforcement Administration and Immigration and Naturalization Service Joint System of Records.

(a) The following system of records is exempted pursuant to provisions of 5 U.S.C. 552a from subsections (c) (3) and (4), (d), (e) (1), (2) and (3), (e)(4) (G), (H), and (I), (e)(5) and (f), (g), and (h) of 5 U.S.C. 552a; in addition the following system of records is exempted pursuant to the provisions of 5 U.S.C. 552 (k)(1) and (k)(2) from subsections (c)(3), (d), (e)(4) (G), (H), and (I), and (f) of 5 U.S.C. 552a.

(1) Automated Intelligence Record System (Pathfinder), JUSTICE/DEA-INS-111.

These exemptions apply to the extent that information in those systems is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(1) and (k)(2).

(b) The system of records listed under paragraph (a) of this section is exempted, for the reasons set forth from the following provisions of 5 U.S.C. 552a:

(1)(c)(3). The release of the disclosure accounting for disclosures made pursuant to subsection (b) of the Act, including those permitted under the routine uses published for these systems of records, would permit the subject of an investigation of an actual or potential criminal, civil or regulatory violation to determine whether he is the subject of investigation, or to obtain information

information concerning the nature of that investigation, and the information obtained, or identity of witnesses and informants and would therefore present a serious impediment to enforcement. In addition, disclosure of the accounting would amount to notice to the individual of the existence of a record; such notice requirement under subsection (f)(1) is specifically exempted for these systems of records.

(2)(c)(4). Since an exemption is being claimed for subsection (d) of the Act (Access to Records), this subsection is inapplicable to the extent that these systems of records are exempted from subsection (d).

(3)(d). Access to the records contained in these systems would inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation of the existence of that investigation, or the nature and scope of the information and evidence obtained as a result of activities, of the identity of witnesses and informants, or would provide information that could enable the subject to avoid detection or apprehension. These factors would present a serious impediment to effective law enforcement because they could prevent the successful completion of the investigation, endanger the physical safety of witnesses or informants, could lead to the improper influencing of witnesses, the destruction of evidence, or the fabrication of testimony.

(4)(e)(1). The notices of these systems of records published in the *Federal Register* set forth the basic statutory or related authority for maintenance of this system. However, in the course of criminal or other law enforcement investigations, cases, and matters, the Immigration and Naturalization Service or the Drug Enforcement Administration will occasionally obtain information concerning actual or potential violations of law that are not strictly within its statutory or other authority or may compile information in the course of an investigation that may not be relevant to a specific prosecution. In the interests of effective law enforcement, it is necessary to retain such information in these systems of records since it can aid in establishing patterns of criminal activity and can provide valuable leads for federal and other law enforcement agencies.

(5)(e)(2). In a criminal investigation or prosecution, the requirement that information be collected to the greatest extent practicable from the subject individual would present a serious impediment to law enforcement because the subject of the investigation or prosecution would be placed on notice as to the existence of the investigation and would therefore be able to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

(6)(e)(3). The requirement that individuals supplying information be provided with a form stating the requirements of subsection (e)(3) would constitute a serious impediment to law enforcement in that it could compromise the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(7)(e)(4) (G) and (H). Since an exemption is being claimed for subsections (f) (Agency Files) and (d) (Access to Records) of the Act these subsections are inapplicable to the extent these systems of records are exempted from subsections (f) and (d).

(8)(e)(4)(I). The categories of sources of the records in these systems have been published in the *Federal Register* in broad generic terms in the belief that this is all that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from disclosure provision is necessary in order to protect the confidentiality of the sources of criminal and law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(9)(e)(5). In the collection of information for criminal law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light and the accuracy of such information can only be determined in a court of law. The restrictions of subsection (e)(5) would restrict the ability of trained investigators, intelligence analysts, and government attorneys in exercising their judgment in reporting on information and investigations and impede the development of criminal or other intelligence necessary for effective law enforcement.

(10)(e)(8). The individual notice requirements of subsection (e)(8) could present a serious impediment to law enforcement as this could interfere with the ability to issue warrants or subpoenas and could reveal investigative techniques, procedures, or evidence.

(11)(f). Procedures for notice to an individual pursuant to subsection (f)(1) as to the existence of records pertaining to him dealing with an actual or potential criminal, civil, or regulatory investigation or prosecution must be exempted because such notice to an individual would be detrimental to the successful conduct and/or completion of an investigation or prosecution pending or future. In addition, mere notice of the fact of an investigation could inform the subject or others that their activities are under or may become the subject of an investigation.

and could enable the subjects to avoid detection or apprehension, to influence witnesses improperly, to destroy evidence, or to fabricate testimony.

Since an exemption is being claimed for subsection (d) of the Act (Access to Records) the required pursuant to subsections (f) (2) through (5) are inapplicable to these systems or records to the extent that these systems of records are exempted from subsection (d).

(12)(g). Since an exemption is being claimed for subsections (d) (Access to Records) and (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for subsections, to the extent that these systems of records are exempted from subsections and (f).

(13)(h). Since an exemption is being claimed for subsection (d) (Access to Records) and (Agency Rules) this section is inapplicable, and is exempted for the reasons set forth for subsections, to the extent that these systems of records are exempted from subsections and (f).

(14) In addition, exemption is claimed for these systems of records from compliance with following provisions of the Privacy Act of 1974 (5 U.S.C. 552a) pursuant to the provision U.S.C. 552a(k)(1): subsections (c)(3), (d), (e)(1), (e)(4) (G), (H), and (I), and (f) to the extent that the records contained in these systems are specifically authorized to be kept secret in the interests of national defense and foreign policy.

[Order No. 742-77, 42 FR 40907, Aug. 12, 1977]

§ 16.103 Exemption of the INTERPOL-United States National Central Bureau (INTERPOL-USNCB) System.

(a) The following system of records is exempt from 5 U.S.C. 552a(c) (3) and (4), (d), (e) and (3), (e)(4) (G) and (H), (e)(5) and (8), (f) and (g):

(1) The INTERPOL-United States National Central Bureau (INTERPOL-USNCB) (Department of Justice) INTERPOL-USNCB Records System (JUSTICE/INTERPOL-001).

This exemption applies only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j)(2), (k)(2), and (k)(5).

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because the release of accounting disclosures would place the subject of an investigation on notice that he is under investigation and provide him with significant information concerning the nature of the investigation, thus resulting in a serious impediment to law enforcement.

(2) From subsections (c)(4), (d), (e)(4) (G), and (H), (f) and (g) because these provisions concern individual access to records and such access might compromise ongoing investigations reveal investigatory techniques and confidential informants, and invade the privacy of private citizens who provide information in connection with a particular investigation.

(3) From subsection (e)(1) because information received in the course of an international criminal investigation may involve a violation of state or local law, and it is beneficial to not release this information to provide investigative leads to state and local law enforcement agencies.

(4) From subsection (e)(2) because collecting information from the subject of criminal investigations would thwart the investigation by placing the subject on notice.

(5) From subsection (e)(3) because supplying an individual with a statement of the intended use of the requested information could compromise the existence of a confidential investigation, and may inhibit cooperation.

(6) From subsection (e)(5) because the vast majority of these records come from local criminal justice agencies and it is administratively impossible to ensure that the records comply with the provision. Submitting agencies are, however, urged on a continuing basis to ensure that records are accurate and include all dispositions.

(7) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to law enforcement by revealing investigatory techniques, procedures, and the existence of confidential investigations.

[Order No. 8–82, 47 FR 44255, Oct. 7, 1982, as amended by Order No. 6–86, 51 FR 15, Apr. 24, 1986]

§ 16.104 Exemption of Office of Special Counsel—Waco System.

(a) The following system of records is exempted from subsections (c)(3) and (4); (d)(1), and (4); (e)(1), (2), (3), (5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (k): CaseLink Document Database for Office of Special Counsel—Waco, JUSTICE/OSC. These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k).

(b) Only that portion of this system which consists of criminal or civil investigatory information is exempted for the reasons set forth from the following subsections:

(1) *Subsection (c)(3)*. To provide the subject of a criminal or civil matter or case under investigation with an accounting of disclosures of records concerning him or her would inform that individual of the existence, nature, or scope of that investigation and thereby seriously impede law enforcement efforts by permitting the record subject and other persons to whom he or she might disclose the records to avoid criminal penalties and civil remedies.

(2) *Subsection (c)(4)*. This subsection is inapplicable to the extent that an exemption is claimed for subsection (d).

(3) *Subsection (d)(1)*. Disclosure of investigatory information could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others.

(4) *Subsection (d)(2)*. Amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden by requiring criminal investigations to be continuously reinvestigated.

(5) *Subsections (d)(3) and (4)*. These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(6) *Subsections (e)(1) and (5)*. It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete; but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide leads in criminal investigations.

(7) *Subsection (e)(2)*. To collect information from the subject individual would serve to notify he or she is the subject of criminal investigative or law enforcement activity and thereby

a serious impediment to law enforcement.

(8) *Subsection (e)(3)*. To inform individuals as required by this subsection would reveal the existence of an investigation and compromise law enforcement efforts.

(9) *Subsection (e)(8)*. To serve notice would give persons sufficient warning to evade law enforcement efforts.

(10) *Subsection (g)*. This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

[Order No. 208–2000, 65 FR 75160, Dec. 1, 2000]

§ 16.105 Exemption of Foreign Terrorist Tracking Task Force System.

(a) The following system of records is exempt from 5 U.S.C. 552a, subsections (c)(3), (c)(2), (3) and (4), and (e)(1) and (4)(I): Flight Training Candidates File System (JUSTICE/FTTTF–001). This exemption applies only to the extent that information is subject to exemption pursuant to 5 U.S.C. 552a(k)(1).

(b) Exemption from the particular subsections is justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting disclosures could reveal information that is classified in the interest of national security.

(2) From subsection (d)(1), (2), (3) and (4) because access to and amendment of certain portions of records within the system would tend to reveal or compromise information classified in the interest of national security.

(3) From subsection (e)(1) because it is often impossible to determine in advance if information obtained will be relevant for the purposes of conducting the risk analysis for flight training candidates.

(4) From subsection (e)(4)(I) to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than have been published in the *Federal Register*. Should the subsection be so interpreted, exemption from this provision is necessary.

because greater specificity concerning the sources of these records could compromise security.

[Order No. 278–2002, 67 FR 51756, Aug. 9, 2002]

§ 16.106 Exemption of the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) Limited Access.

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d)(1), (d)(2) and (4), (e)(1), (2), and (3), (e)(4)(G), (H) and (I), (e)(5) and (8), (f) and (g).

(1) Criminal Investigation Report System (JUSTICE/ATF–003).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, ATF may waive the application of the exemption.

(b) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting disclosures from records concerning him/her would reveal investigative interest not only in the record subject but also of the recipient agency. This would permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses or flee the country to avoid the thrust of the investigation.

(2) From subsection (c)(4) because an exemption being claimed for subsection (d) makes subsection (c)(4) inapplicable.

(3) From subsections (d)(1), (e)(4)(G) and (H), (f) and (g) because these provisions concerning individual access to investigative records, compliance with which could compromise sensitive information, interfere with the overall law enforcement process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information, including accounting information, which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety of law enforcement personnel.

(4) From subsection (d)(2) because, due to the nature of the information collected and the essential length of time it is maintained, to require ATF to amend information thought to be incorrect, irrelevant or untimely, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to answer questions of accuracy, etc.

(5) From subsections (d)(3) and (4) because these subsections are inapplicable to the exemption is claimed from (d)(1) and (2).

(6) From subsection (e)(1) because: (i) It is not possible in all instances to determine relevance or necessity of specific information in the early stages of a criminal or other investigation.

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity in a specific investigative activity can be established.

(iii) In any investigation, ATF might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or to another investigative activity under the jurisdiction of another agency.

(7) From subsection (e)(2) because the nature of criminal and other investigative activities is such that vital information about an individual can only be obtained from other persons familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(8) From subsection (e)(3) because disclosure would provide the subject with substantial information that could impede or compromise the investigation. The individual could seek to interfere with undercover investigative activities and could take steps to evade the investigation or flee a specific area.

(9) From subsection (e)(4)(I) because the categories of sources of the records in these systems have been published in the *Federal Register* in broad generic terms in the belief that this meets the requirements of that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(10) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restriction imposed by subsection (e)(5) would restrict the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement.

(11) From subsection (e)(8) because the notice requirements of this provision could seriously interfere with a law enforcement activity by alerting the subject of a criminal or other investigation of existing investigative interest.

(c) The following system of records is exempt from 5 U.S.C. 552a(c)(3), (d)(1), (2), (3) and (e)(1), (e)(4)(G), (H) and (I), and (f).

(1) Internal Security Record System (JUSTICE/ATF-006).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2) and (k)(5). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, ATF may waive the applicable exemption.

(d) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because to provide the subject with an accounting of disclosed records in this system could inform that individual of the existence, nature, or scope of an actual or potential law enforcement investigation, and thereby seriously impede law enforcement efforts by permitting the record subject and other persons to whom he might

disclose the records to avoid criminal penalties, civil remedies, or other measures.

(2) From subsection (d)(1) because disclosure of records in the system could reveal the identity of confidential sources and result in an unwarranted invasion of the privacy of others. Disclosure may also reveal information relating to actual or potential criminal investigations. Such breaches would restrict the free flow of information which is vital to the law enforcement process and the determination of an applicant's qualifications.

(3) From subsection (d)(2) because, due to the nature of the information collected and the essential length of time it is maintained, to require ATF to amend information thought to be incorrect, irrelevant or untimely, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to answer questions of accuracy, etc.

(4) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent an exemption is claimed from (d)(1) and (2).

(5) From subsection (e)(1) because it is often impossible to determine in advance if investigative records contained in this system are accurate, relevant, timely, complete, and provide some assistance to either effective law enforcement investigations, or to the determination of the qualifications and suitability of an applicant. It also is necessary to retain this information as an aid in establishing patterns of activity and provide investigative leads. Information that may appear irrelevant, when combined with other apparently irrelevant information, can often provide a composite picture of a subject or an applicant which assists the law enforcement process and the determination of an applicant's suitability qualifications.

(6) From subsection (e)(4)(G) and (H), and (f) because these provisions concern individual access to investigative records, compliance with which could compromise sensitive information and interfere with the overall law enforcement or qualification process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual's personal privacy, reveal sensitive investigative technique, or constitute a potential danger to the health or safety of law enforcement personnel. In addition, disclosure of information collected pursuant to an employment suitability or similar inquiry could reveal the identity of a source who provided information under an express promise of confidentiality, or could compromise the objectivity and fairness of a testing or examination process.

(7) From subsection (e)(4)(I) because the categories of sources of the records in these systems have been published in the *Federal Register* in broad generic terms in the belief that this meets the requirements of that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(e) The following system of records is exempt from 5 U.S.C. 552a(c)(3), (d)(1), (2), (3) and (e)(1), (e)(4)(G), (H) and (I), and (f).

(1) Personnel Record System (JUSTICE/ATF-007).

(2) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(5). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, ATF may waive the application of the exemption.

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting disclosures from records concerning him/her would reveal the existence, nature, or scope of actual or potential personnel action. This would permit the record subject to take measures to hamper or impede such actions.

(2) From subsections (d)(1), (e)(4)(G) and (H), and (f) because many persons are contacted who, without an assurance of anonymity, refuse to provide information concerning a candidate for a position with ATF. Access could reveal the identity of the source of the information and constitute a breach of the promise of confidentiality on the part of ATF. Such breaches ultimately would restrict the free flow of information vital to a determination of a candidate's qualifications and suitability.

(3) From subsection (d)(2) because, due to the nature of the information collected and the essential length of time it is maintained, to require ATF to amend information thought to be incorrect, irrelevant or untimely, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to

questions of accuracy, etc.

(4) From subsections (d)(3) and (4) because these subsections are inapplicable to the exemption is claimed from (d)(1) and (2).

(5) From subsection (e)(1) because:

(i) It is not possible in all instances to determine relevancy or necessity of specific information in the early stages of a personnel-related action.

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity in a specific investigative activity can be established.

(iii) ATF might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or to another investigative activity under the jurisdiction of another agency.

(6) From subsection (e)(4)(I) because the categories of sources of the records in these systems have been published in the *Federal Register* in broad generic terms in the belief that this meets that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of sources of criminal and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

(g) The following systems of records are exempt from 5 U.S.C. 552a(c)(3), (d)(1), (2), (3), (4), (e)(1), (e)(4)(G), (H) and (I), and (f).

(1) Regulatory Enforcement Record System (JUSTICE/ATF-008).

(2) Technical and Scientific Services Record System (JUSTICE/ATF-009).

(3) These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2). Where compliance would not appear to interfere with or adversely affect the overall law enforcement process, ATF may waive the applicable exemption.

(h) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3) because making available to a record subject the accounting disclosures from records concerning him/her would reveal investigative interest, whether criminal or regulatory, not only of ATF, but also of the recipient agency. This would permit record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses or flee the area to avoid the thrust of the investigation thus seriously hampering the regulatory and law enforcement functions of ATF.

(2) From subsections (d)(1), (e)(4)(G) and (H), and (f) because these provisions concern individual access to investigative and compliance records, disclosure of which could compromise sensitive information, interfere with the overall law enforcement and regulatory process by revealing a pending sensitive investigation, possibly identify a confidential source, disclose information, including actual or potential tax information, which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety of law enforcement personnel.

(3) From subsection (d)(2) because, due to the nature of the information collected and the essential length of time it is maintained, to require ATF to amend information thought to be incorrect, irrelevant or untimely, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations and compliance actions attempting to resolve questions of accuracy, etc.

(4) From subsections (d)(3) and (4) because these subsections are inapplicable to the exemption is claimed from (d)(1) and (2).

(5) From subsection (e)(1) because:

(i) It is not possible in all instances to determine relevancy or necessity of specific information in the early stages of a criminal, civil, regulatory, or other investigation.

(ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity in a specific investigative or regulatory activity can be established.

(iii) In any investigation or compliance action ATF might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement dissemination will be made to the agency charged with enforcing such law.

(iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or compliance action or to an investigative activity under the jurisdiction of another agency.

(6) From subsection (e)(4)(I) because the categories of sources of the records in these systems have been published in the *Federal Register* in broad generic terms in the belief that this meets the requirements that subsection (e)(4)(I) of the Act requires. In the event, however, that this subsection should be interpreted to require more detail as to the identity of sources of the records in these systems, exemption from this provision is necessary in order to protect the confidentiality of the sources of criminal, regulatory, and other law enforcement information. Such exemption is further necessary to protect the privacy and physical safety of witnesses and informants.

[Order No. 002–2003, 68 FR 3393, Jan. 24, 2003]

§ 16.130 Exemption of Department of Justice Systems: Correspondence Management Systems for the Department of Justice (DOJ-003); Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Requests and Administrative Appeals for the Department of Justice (DOJ-004).

(a) The following Department of Justice systems of records are exempted from subsections (c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1), (2), (3), (5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j) and (k). These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k).

(1) Correspondence Management Systems (CMS) for the Department of Justice (DOJ), DOJ/003.

(2) Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records and Administrative Appeals for the Department of Justice (DOJ), DOJ/004.

(b) These systems are exempted for the reasons set forth from the following subsection

(1) *Subsection (c)(3)*. To provide the subject of a criminal, civil, or counterintelligence matter under investigation with an accounting of disclosures of records concerning him or her could inform that individual of the existence, nature, or scope of that investigation, and thus seriously impede law enforcement or counterintelligence efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties, civil remedies, or counterintelligence measures.

(2) *Subsection (c)(4)*. This subsection is inapplicable to the extent that an exemption is claimed for subsection (d).

(3) *Subsection (d)(1)*. Disclosure of investigatory information could interfere with the investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others. Disclosure of classified national security information would cause damage to the national security of the United States.

(4) *Subsection (d)(2)*. Amendment of the records would interfere with ongoing criminal or law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(5) *Subsections (d)(3) and (4)*. These subsections are inapplicable to the extent exemptions claimed from (d)(1) and (2).

(6) *Subsection (e)(1)*. It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interest of effective law enforcement and counterintelligence, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(7) *Subsection (e)(2)*. To collect information from the subject individual could serve notice

he or she is the subject of a criminal investigation and thereby present a serious impediment to such investigations.

(8) *Subsection (e)(3)*. To inform individuals as required by this subsection could reveal the existence of a criminal investigation and compromise investigative efforts.

(9) *Subsection (e)(5)*. It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interest of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(10) *Subsection (e)(8)*. To serve notice could give persons sufficient warning to evade investigative efforts.

(11) *Subsection (g)*. This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

[Order No. 241–2001, 66 FR 41445, Aug. 8, 2001; 66 FR 43308, Aug. 17, 2001]

§ 16.131 Exemption of Department of Justice (DOJ)/Nationwide Joint Automated Booking System (JABS), DOJ-005.

(a) The following system of records is exempt from 5 U.S.C. 552a(c)(3) and (4), (d), (e)(3), (4)(G) and (H), (e)(5) and (8), (f) and (g): Nationwide Joint Automated Booking System, Department of Justice/DOJ-005. These exemptions apply only to the extent that information in the system is subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). Where compliance would interfere with or adversely affect the law enforcement process, the DOJ may waive the exemptions, either partially or totally.

(b) Exemption from the particular subsections are justified for the following reasons:

(1) From subsections (c)(3), (c)(4), and (d) to the extent that access to records in this system may impede or interfere with law enforcement efforts, result in the disclosure of information that would constitute an unwarranted invasion of the personal privacy of collection record subjects or other third parties, and/or jeopardize the health and/or safety of third parties.

(2) From subsection (e)(1) to the extent that it is necessary to retain all information in or

to impede, compromise, or interfere with law enforcement efforts, e.g., where the significance of the information may not be readily determined and/or where such information may provide leads or assistance to Federal and other law enforcement agencies in discharging their enforcement responsibilities.

(3) From subsection (e)(2) because, in some instances, the application of this provision presents a serious impediment to law enforcement since it may be necessary to obtain and verify information from a variety of sources other than the record subject to ensure safekeeping, security, and effective law enforcement. For example, it may be necessary for medical and psychiatric personnel to provide information regarding the subject's behavior, physical health, or mental stability, etc. to ensure proper care while in custody, or it may be necessary to obtain information from a case agent or the court to ensure proper disposition of the subject individual.

(4) From subsection (e)(3) because the requirement that agencies inform each individual that it asks to supply information of such information as is required by subsection (e)(3) may, in some cases, impede the information gathering process or otherwise interfere with or compromise law enforcement efforts, e.g., the subject may deliberately withhold information or give erroneous information.

(5) From subsection (4)(G) and (H) because the application of these provisions would present a serious impediment to law enforcement efforts.

(6) From subsection (e)(5) because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance and the accuracy of such information can only be determined by the court of law. The restrictions imposed by subsection (e)(5) would restrict the ability to collect information for law enforcement purposes, may prevent the eventual development of the necessary criminal intelligence, or otherwise impede law enforcement or delay trained law enforcement personnel from timely exercising their judgment in managing the arrestee.

(7) From subsection (e)(8) to the extent that such notice may impede, interfere with, or otherwise compromise law enforcement and security efforts.

(8) From subsection 5 U.S.C. 552a(f) to the extent that compliance with the requirements of procedures providing individual access to records, compliance could impede, compromise

interfere with law enforcement efforts.

(9) From subsection (g) to the extent that this system is exempt from the access and amendment provisions of subsection (d).

[Order No. 242–2001, 66 FR 41445, Aug. 8, 2001; 66 FR 44308, Aug. 17, 2001]

§ 16.132 Exemption of Department of Justice System—Personnel Investigation and Clearance Records for the Department of Justice (DOJ), DOJ-006.

(a) The following Department of Justice system of records is exempted from subsections (b) and (4); (d)(1), (2), (3) and (4); (e)(1),(2),(3),(5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j) and (k): Personnel Investigation and Security Clearance Records for the Department of Justice (DOJ), DOJ-006. These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j) and (k).

(b) Exemption from the particular subsections is justified for the following reasons:

(1) *Subsection (c)(3)*. To provide the subject with an accounting of disclosures of record system could inform that individual of the existence, nature, or scope of an actual or potential law enforcement or counterintelligence investigation, and thereby seriously impede law enforcement or counterintelligence efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties, civil remedies, or counterintelligence measures.

(2) *Subsection (c)(4)*. This subsection is inapplicable to the extent that an exemption is claimed for subsection (d).

(3) *Subsection (d)(1)*. Disclosure of records in the system could reveal the identity of confidential sources and result in an unwarranted invasion of the privacy of others. Disclosure may also reveal information relating to actual or potential criminal investigations. Disclosure of classified national security information would cause damage to the national security of the United States.

(4) *Subsection (d)(2)*. Amendment of the records could interfere with ongoing criminal or law enforcement proceedings and impose an impossible administrative burden by requiring

investigations to be continuously reinvestigated.

(5) *Subsections (d)(3) and (4)*. These subsections are inapplicable to the extent exempti claimed from (d)(1) and (2).

(6) *Subsection (e)(1)*. It is often impossible to determine in advance if investigatory recor contained in this system are accurate, relevant, timely and complete, but, in the interest effective law enforcement and counterintelligence, it is necessary to retain this informati aid in establishing patterns of activity and provide investigative leads.

(7) *Subsection (e)(2)*. To collect information from the subject individual could serve notic he or she is the subject of a criminal investigation and thereby present a serious impedi such investigations.

(8) *Subsection (e)(3)*. To inform individuals as required by this subsection could reveal t existence of a criminal investigation and compromise investigative efforts.

(9) *Subsection (e)(5)*. It is often impossible to determine in advance if investigatory recor contained in this system are accurate, relevant, timely and complete, but, in the interest effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(10) *Subsection (e)(8)*. To serve notice could give persons sufficient warning to evade investigative efforts.

(11) *Subsection (g)*. This subsection is inapplicable to the extent that the system is exen from other specific subsections of the Privacy Act.

[Order No. 297–2002, 67 FR 70163, Nov. 21, 2002]

§ 16.133 Exemption of Department of Justice Regional Data Exchange System (RDE. DOJ–012.

(a) The Department of Justice Regional Data Exchange System (RDEX), DOJ–012, is exempted from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (5), an and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). These exemptions apply only

extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j)(4).

(b) This system is exempted from the following subsections for the reasons set forth below:

(1) From subsection (c)(3) because making available to a record subject the accounting disclosures of criminal law enforcement records concerning him or her could inform that individual of the existence, nature, or scope of an investigation, or could otherwise seriously impede law enforcement efforts.

(2) From subsection (c)(4) because this system is exempt from subsections (d)(1), (2), and (4).

(3) From subsection (d)(1) because disclosure of criminal law enforcement information could interfere with an investigation, reveal the identity of confidential sources, and result in an unwarranted invasion of the privacy of others.

(4) From subsection (d)(2) because amendment of the records would interfere with ongoing criminal law enforcement proceedings and impose an impossible administrative burden requiring investigations to be continuously reinvestigated.

(5) From subsections (d)(3) and (4) because these subsections are inapplicable to the extent that exemption is claimed from subsections (d)(1) and (2).

(6) From subsection (e)(1) because it is often impossible to determine in advance if criminal law enforcement records contained in this system are relevant and necessary, but, in the interest of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(7) From subsection (e)(2) because collecting information from the subject individual could serve notice that he or she is the subject of a criminal law enforcement matter and thereby present a serious impediment to law enforcement efforts. Further, because of the nature of criminal law enforcement matters, vital information about an individual frequently can be obtained only from other persons who are familiar with the individual and his or her activities, and it often is not practicable to rely on information provided directly by the individual.

(8) From subsection (e)(3) because informing individuals as required by this subsection

reveal the existence of a criminal law enforcement matter and compromise criminal law enforcement efforts.

(9) From subsection (e)(5) because it is often impossible to determine in advance if criminal enforcement records contained in this system are accurate, relevant, timely, and complete. In the interests of effective law enforcement, it is necessary to retain this information to establish patterns of activity and obtaining investigative leads.

(10) From subsection (e)(8) because serving notice could give persons sufficient warning to evade criminal law enforcement efforts.

(11) From subsection (g) to the extent that this system is exempt from other specific subsections of the Privacy Act.

[Order No. 007–2005, 70 FR 49870, Aug. 25, 2005]

[\[TOP\]](#)

Title 28—Judicial Administration

Chapter V—Bureau of Prisons

PART 513—ACCESS TO RECORDS

Subpart D—Release of Information

General Provisions and Procedures

513.30 Purpose and scope.

513.31 Limitations.

513.32 Guidelines for disclosure.

513.33 Production of records in court.

513.34 Protection of individual privacy—disclosure of records to third parties.

513.35 Accounting/nonaccounting of disclosures to third parties.

513.36 Government contractors.

Inmate Requests to Institution for Information

513.40 Inmate access to Inmate Central File.

513.41 Inmate access to Inmate Central File in connection with parole hearings.

513.42 Inmate access to medical records.

513.43 Inmate access to certain Bureau Program Statements.

513.44 Fees for copies of Inmate Central File and Medical Records.

Privacy Act Requests for Information

513.50 Privacy Act requests by inmates.

Freedom of Information Act Requests for Information

513.60 Freedom of Information Act requests.

513.61 Freedom of Information Act requests by inmates.

513.62 Freedom of Information Act requests by former inmates.

513.63 Freedom of Information Act requests on behalf of an inmate or former inmate.

513.64 Acknowledgment of Freedom of Information Act requests.

513.65 Review of documents for Freedom of Information Act requests.

513.66 Denials and appeals of Freedom of Information Act requests.

513.67 Fees for Freedom of Information Act requests.

513.68 Time limits for responses to Freedom of Information Act requests.

Authority: 5 U.S.C. 301, 552, 552a; 13 U.S.C.; 18 U.S.C. 3621, 3622, 3624, 4001, 4042, 4082 (Repealed in part as to conduct occurring on or after November 1, 1987), 5006–5007 (Repealed October 12, 1984, as to conduct occurring after that date), 5039; 28 U.S.C. 504; 31 U.S.C. 3711(f); 5 CFR part 297; 28 CFR 0.95–0.99 and parts 16 and 301.

Source: 45 FR 44228, June 30, 1980, unless otherwise noted.

Subpart D—Release of Information

Source: 61 FR 64950, Dec. 9, 1996, unless otherwise noted.

General Provisions and Procedures

§ 513.30 Purpose and scope.

This subpart establishes procedures for the release of requested records in possession of the Federal Bureau of Prisons ("Bureau"). It is intended to implement provisions of the Freedom of Information Act (FOIA), 5 U.S.C. 552, and the Privacy Act, 5 U.S.C. 552a, and to supplement Department of Justice (DOJ) regulations concerning the production or disclosure of records, 28 CFR part 16.

§ 513.31 Limitations.

(a) *Social Security Numbers.* As of September 27, 1975, Social Security Numbers may not be used in their entirety as a method of identification for any Bureau record system, unless such use is authorized by statute or by regulation adopted prior to January 1, 1975.

(b) *Employee records.* Access and amendment of employee personnel records under the Privacy Act are governed by Office of Personnel Management regulations published in 5 CFR part 297 and by Department of Justice regulations published in 28 CFR part 16.

§ 513.32 Guidelines for disclosure.

The Bureau provides for the disclosure of agency information pursuant to applicable law, the Freedom of Information Act (5 U.S.C. 552), and the Privacy Act (5 U.S.C. 552a).

§ 513.33 *Production of records in court.*

Bureau records are often sought by subpoena, court order, or other court demand, in connection with court proceedings. The Attorney General has directed that these records not be produced in court without the approval of the Attorney General or his or her designee. The guidelines are set forth in 28 CFR part 16, subpart B.

§ 513.34 *Protection of individual privacy—disclosure of records to third parties.*

(a) Information that concerns an individual and is contained in a system of records maintained by the Bureau shall not be disclosed to any person, or to another agency except under the provisions of the Privacy Act, 5 U.S.C. 552a, the Freedom of Information Act, 5 U.S.C. 552, and Departmental regulations.

(b) Lists of Bureau inmates shall not be disclosed.

§ 513.35 *Accounting/nonaccounting of disclosures to third parties.*

Accounting/nonaccounting of disclosures to third parties shall be made in accordance with the Department of Justice regulations contained in 28 CFR 16.52.

§ 513.36 *Government contractors.*

(a) No Bureau component may contract for the operation of a record system by or on behalf of the Bureau without the express written approval of the Director or the Director's designee.

(b) Any contract which is approved shall contain the standard contract requirements promulgated by the General Services Administration (GSA) to ensure compliance with the requirements imposed by the Privacy Act. The contracting component shall have the responsibility to ensure that the contractor complies with the contract requirements relating to privacy.

Inmate Requests to Institution for Information

§ 513.40 Inmate access to Inmate Central File.

Inmates are encouraged to use the simple access procedures described in this section to review disclosable records maintained in his or her Inmate Central File, rather than the procedures described in §§ 513.60 through 513.68 of this subpart. Disclosable records in the Inmate Central File include, but are not limited to, documents relating to the inmate's sentence, detainer, participation in Bureau programs such as the Inmate Financial Responsibility Program, classification data, parole information, mail, visits, property, conduct, work, release processing, and general correspondence. This information is available without filing a Freedom of Information Act request. If any information is withheld from the inmate, staff will provide the inmate with a general description of that information and also will notify the inmate that he or she may file a Freedom of Information Act request.

(a) *Inmate review of his or her Inmate Central File.* An inmate may at any time request to review all disclosable portions of his or her Inmate Central File by submitting a request to a staff member designated by the Warden. Staff are to acknowledge the request and schedule a review of the file with the inmate, as promptly as is practical, for a review of the file at a time which will not disrupt institution operations.

(b) *Procedures for inmate review of his or her Inmate Central File.* (1) Prior to the inmate review of the file, staff are to remove the Privacy Folder which contains documents withheld from disclosure pursuant to § 513.32.

(2) During the file review, the inmate is to be under direct and constant supervision by staff. The staff member monitoring the review shall enter the date of the inmate's file review on the Inmate Activity Record and initial the entry. Staff shall ask the inmate to initial the entry and if the inmate refuses to do so, shall enter a notation to that effect.

(3) Staff shall advise the inmate if there are documents withheld from disclosure and, if so, shall advise the inmate of the inmate's right under the provisions of § 513.61 to make a request for the withheld documents.

§ 513.41 Inmate access to Inmate Central File in connection with parole hearings.

A parole-eligible inmate (an inmate who is currently serving a sentence for an offense committed prior to November 1, 1987) may review disclosable portions of the Inmate Central File.

File prior to the inmate's parole hearing, under the general procedures set forth in § 513.40, in addition, the following guidelines apply:

(a) A parole-eligible inmate may request to review his or her Inmate Central File by submitting the appropriate Parole Commission form. This form ordinarily shall be available to each inmate within five work days after a list of eligible inmates is prepared.

(b) Bureau staff ordinarily shall schedule an eligible inmate for a requested Inmate Central File review within seven work days of the request after the inmate has been scheduled for a parole hearing. A reasonable extension of time is permitted for documents which have been pending (prior to the inmate's request) to originating agencies for clearance, or which are otherwise unavailable at the institution.

(c) A report received from another agency which is determined to be nondisclosable (see § 513.40(b)) will be summarized by that agency, in accordance with Parole Commission regulations. Bureau staff shall place the summary in the appropriate disclosable section of the Inmate Central File. The original report (or portion which is summarized in another document) will be placed in the portion of the Privacy File for Joint Use by the Bureau and the Parole Commission.

(d) Bureau documents which are determined to be nondisclosable to the inmate will be summarized for the inmate's review. A copy of the summary will be placed in the disclosable section of the Inmate Central File. The document from which the summary is taken will be placed in the Joint Use Section of the Privacy Folder. Nondisclosable documents not summarized for the inmate's review are not available to the Parole Commission and are placed in a nondisclosable section of the Inmate Central File.

(e) When no response regarding disclosure has been received from an originating agency at the time for inmate review prior to the parole hearing, Bureau staff are to inform the Parole Commission Hearing Examiner.

§ 513.42 Inmate access to medical records.

(a) Except for the limitations of paragraphs (c) and (d) of this section, an inmate may review his or her medical records from his or her medical file (including dental records) by submitting a request to a staff member designated by the Warden.

(b) Laboratory reports which contain only scientific testing results and which contain no evaluation or opinion (such as Standard Form 514A, Urinalysis) are ordinarily disclosable. Results of HIV testing may be reviewed by the inmate. However, an inmate may not retain a copy of his or her test results while the inmate is confined in a Bureau facility or a Comr Corrections Center. A copy of an inmate's HIV test results may be forwarded to a third party outside the institution and chosen by the inmate, provided that the inmate gives written authorization for the disclosure.

(c) Medical records containing subjective evaluations and opinions of medical staff relating to the inmate's care and treatment will be provided to the inmate only after the staff review required by paragraph (d) of this section. These records include, but are not limited to, outpatient notes, consultation reports, narrative summaries or reports by a specialist, or reports by the physician, summaries by specialists as the result of laboratory analysis, or in-patient progress reports.

(d) Prior to release to the inmate, records described in paragraph (c) of this section shall be reviewed by staff to determine if the release of this information would present a harm to the inmate or other individuals. Any records determined not to present a harm will be released to the inmate at the conclusion of the review by staff. If any records are determined by staff not to be releasable based upon the presence of harm, the inmate will be so advised in writing and provided the address of the agency component to which the inmate may address a formal request for the withheld records. An accounting of any medical records will be maintained in the inmate's medical file.

§ 513.43 Inmate access to certain Bureau Program Statements.

Inmates are encouraged to use the simple local access procedures described in this section to review certain Bureau Program Statements, rather than the FOIA procedures described in §§ 513.60 through 513.68 of this subpart.

(a) For a current Bureau Program Statement containing rules (regulations published in the *Federal Register* and codified in 28 CFR), local access is available through the institution library.

(b) For a current Bureau Program Statement not containing rules (regulations published in the *Federal Register* and codified in 28 CFR), inmates may request that it be placed in the

institution law library. Placement of a requested Program Statement in the law library is the discretion of the Warden, based upon local institution conditions.

(c) Inmates are responsible for the costs of making personal copies of any Program Statement maintained in the institution law library. For copies of Program Statements obtained under FOIA procedures described in §§ 513.60 through 513.68 of this subpart, fees will be calculated in accordance with 28 CFR 16.10.

§ 513.44 Fees for copies of Inmate Central File and Medical Records.

Within a reasonable time after a request, Bureau staff are to provide an inmate person a copy of requested disclosable documents maintained in the Inmate Central File and Medical Records. Fees for the copies are to be calculated in accordance with 28 CFR 16.10.

Privacy Act Requests for Information

§ 513.50 Privacy Act requests by inmates.

Because inmate records are exempt from disclosure under the Privacy Act (see 28 CFR 16.10), inmate requests for records under the Privacy Act will be processed in accordance with FOIA. See §§ 513.61 through 513.68.

Freedom of Information Act Requests for Information

§ 513.60 Freedom of Information Act requests.

Requests for any Bureau record (including Program Statements and Operations Memoranda) ordinarily shall be processed pursuant to the Freedom of Information Act, 5 U.S.C. 552. A request must be made in writing and addressed to the Director, Federal Bureau of Prisons, First Street, NW., Washington, D.C. 20534. The requester shall clearly mark on the face of the letter and the envelope "FREEDOM OF INFORMATION REQUEST," and shall clearly identify the records sought. See §§ 513.61 through 513.63 for additional requirements.

§ 513.61 Freedom of Information Act requests by inmates.

(a) Inmates are encouraged to use the simple access procedures described in § 513.40 to review disclosable records maintained in his or her Inmate Central File.

(b) An inmate may make a request for access to documents in his or her Inmate Central Medical File (including documents which have been withheld from disclosure during the inmate's review of his or her Inmate Central File pursuant to § 513.40) and/or other documents concerning the inmate which are not contained in the Inmate Central File or Medical File shall process such a request pursuant to the applicable provisions of the Freedom of Information Act, 5 U.S.C. 552.

(c) The inmate requester shall clearly mark on the face of the letter and on the envelope "FREEDOM OF INFORMATION ACT REQUEST" , and shall clearly describe the record sought, including the approximate dates covered by the record. An inmate making such request must provide his or her full name, current address, date and place of birth. In addition, if the inmate requests documents to be sent to a third party, the inmate must provide with the request an example of his or her signature, which must be verified and dated within three months of the date of the request.

§ 513.62 Freedom of Information Act requests by former inmates.

Former federal inmates may request copies of their Bureau records by writing to the Director, Federal Bureau of Prisons, 320 First Street, NW., Washington, D.C. 20534. Such request shall be processed pursuant to the provisions of the Freedom of Information Act. The request must be clearly marked on the face of the letter and on the envelope "FREEDOM OF INFORMATION ACT REQUEST" , and must describe the record sought, including the approximate dates covered by the record. A former inmate making such a request must provide his or her full name, current address, date and place of birth. In addition, the requester must provide with the request an example of his or her signature, which must be either notarized or sworn under penalty of perjury, and dated within three (3) months of the date of the request.

§ 513.63 Freedom of Information Act requests on behalf of an inmate or former inmate.

A request for records concerning an inmate or former inmate made by an authorized representative of that inmate or former inmate will be treated as in § 513.61, on receipt of the inmate's or former inmate's written authorization. This authorization must be dated within three (3) months of the date of the request letter. Identification data, as listed in 28 CFR 16.4, must be provided.

§ 513.64 Acknowledgment of Freedom of Information Act requests.

(a) All requests for records under the Freedom of Information Act received by the FOI/P Administrator, Office of General Counsel, will be reviewed and may be forwarded to the appropriate Regional Office for proper handling. Requests for records located at a Bureau facility other than the Central Office or Regional Office may be referred to the appropriate facility at that facility for proper handling.

(b) The requester shall be notified of the status of his or her request by the office with final responsibility for processing the request.

§ 513.65 Review of documents for Freedom of Information Act requests.

If a document is deemed to contain information exempt from disclosure, any reasonably segregable portion of the record shall be provided to the requester after deletion of the exempt portions. If documents, or portions of documents, in an Inmate Central File have been determined to be nondisclosable by institution staff but are later released by Regional or Central Office staff pursuant to a request under this section, appropriate instructions will be given to the institution to move those documents, or portions, from the Inmate Privacy File into the disclosable section of the Inmate Central File.

§ 513.66 Denials and appeals of Freedom of Information Act requests.

If a request made pursuant to the Freedom of Information Act is denied in whole or in part, a denial letter must be issued and signed by the Director or his or her designee, and shall state the basis for denial under § 513.32. The requester who has been denied such access shall be advised that he or she may appeal that decision to the Office of Information and Privacy, Department of Justice, Suite 570, Flag Building, Washington, D.C. 20530. Both the envelope and the letter of appeal itself should be clearly marked: "Freedom of Information Act Appeal".

§ 513.67 Fees for Freedom of Information Act requests.

Fees for copies of records disclosed under the FOIA, including fees for a requester's own copies of records, may be charged in accordance with Department of Justice regulations contained in 28 CFR 16.10.

§ 513.68 Time limits for responses to Freedom of Information Act requests.

Consistent with sound administrative practice and the provisions of 28 CFR 16.1, the Bureau

strives to comply with the time limits set forth in the Freedom of Information Act.

[\[TOP\]](#)

Title 45—Public Welfare

Chapter V—Foreign Claims Settlement Commission

PART 503—PRIVACY ACT AND GOVERNMENT IN THE SUNSHINE REGULATIONS

Subpart A—Privacy Act Regulations

Sec.

503.1 Definitions—Privacy Act.

503.2 General policies—Privacy Act.

503.3 Conditions of disclosure.

503.4 Accounting of certain disclosures.

503.5 Access to records or information.

503.6 Determination of requests for access to records.

503.7 Amendment of a record.

503.8 Appeals from denial of requests for amendment to records.

503.9 Fees.

503.10 Exemptions.

503.11 Reports.

503.12 Notices.

Authority: 5 U.S.C. 552a(f).

Source: 66 FR 49844, Oct. 1, 2001, unless otherwise noted.

Subpart A—Privacy Act Regulations

§ 503.1 Definitions—Privacy Act.

For the purpose of this part:

Agency includes any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government (including the Executive Office of the President) or any independent regulatory agency. The Foreign Claims Settlement Commission ("Commission") is an *agency* with the meaning of the term.

Individual means a citizen of the United States or an alien lawfully admitted for permanent residence.

Maintain includes maintain, collect, use or disseminate.

Record means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, an individual's education, financial transactions, medical history, and criminal or employment history, and that contains an individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Routine use means, with respect to the disclosure of a record, the use of that record for a purpose which is compatible with the purpose for which it was collected.

Statistical record means a record in a system of records maintained for statistical research reporting purposes only and not used in whole or in part in making any determination about an identifiable individual except as provided by section 13 U.S.C. 8.

System of records means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol,

other identifying particular assigned to the individual.

§ 503.2 General policies—Privacy Act.

The Commission will protect the privacy of an individual identified in any information or systems which it maintains. Accordingly, its officials and employees, except as otherwise provided by law or regulation, will:

- (a) Permit an individual to determine what records pertaining to that individual are collected, maintained, used or disseminated by the Commission.
- (b) Permit an individual to prevent a record pertaining to that individual obtained by the Commission for a particular purpose from being used or made available for another purpose without the individual's consent.
- (c) Permit an individual to gain access to information pertaining to that individual in Commission records, to have a copy made of all or any portion thereof, and to correct or amend those records.
- (d) Collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that the Commission's action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of the information.
- (e) Permit exemptions from record requirements provided under the Privacy Act only when an important public policy use for the exemption has been determined in accordance with the statutory authority.

§ 503.3 Conditions of disclosure.

The Commission will not disclose any record contained in a system of records by any means of communication to any person or any other agency except by written request of or prior written consent of the individual to whom the record pertains unless the disclosure is:

- (a) To those officers and employees of the Commission who have a need for the record in the performance of their duties;

(b) Required under the Freedom of Information Act, 5 U.S.C. 552;

(c) For a routine use;

(d) To the Bureau of Census for purposes of planning or carrying out a census or survey related activity under the provisions of Title 13, United States Code;

(e) To a recipient who has provided the Commission with adequate advance assurance record will be used solely as a statistical research or reporting record, and the record is transferred in a form that is not individually identifiable;

(f) To the National Archives of the United States as a record which has sufficient historic or other value to warrant its continued preservation by the United States Government or for evaluation to determine whether the record has that value;

(g) To another agency or to an instrumentality of any government jurisdiction within or under control of the United States for a civil or criminal law enforcement activity authorized by law, provided the head of the agency or instrumentality has made a prior written request to the Commission, specifying the particular record and the law enforcement activity for which sought;

(h) To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if, upon disclosure, notification is transmitted to the last known address of the individual;

(i) To either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of the joint committee;

(j) To the Comptroller General, or any of that official's authorized representatives, in the course of the performance of the duties of the General Accounting Office; or

(k) Pursuant to the order of a court of competent jurisdiction.

§ 503.4 Accounting of certain disclosures.

(a) Except for disclosures under § 503.3(a) and (b) of this part, the Administrative Office keep an accurate accounting of each disclosure of a record to any person or to another made under § 503.3(c), (d), (e), (f), (g), (h), (i), (j), and (k) of this part.

(b) Except for a disclosure made to another agency or to an instrumentality of any governmental jurisdiction under § 503.3(g) of this part, the Administrative Officer will make accounting as required under paragraph (a) of this section available to any individual upon written request made in accordance with § 503.5.

(c) The Administrative Officer will inform any person or other agency about any correction or notation of dispute made in accordance with § 503.7 of this part of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

(d) An accounting of disclosures of records within this section will consist of the date, name, the purpose of each disclosure of a record to any person or to another agency, and the name and address of the person or agency to whom the disclosure is made.

(e) This accounting shall be retained for 5 years or the life of the record, whichever is longer, after the disclosure for which the accounting is made.

§ 503.5 Access to records or information.

(a) Upon request in person or by mail, any individual will be informed whether or not a set of records maintained by the Commission contains a record or information pertaining to that individual.

(b) Any individual requesting access to a record or information in person must appear in person at the offices of the Foreign Claims Settlement Commission, 600 E Street, NW., Room 600, Washington, DC, between the hours of 9 a.m. and 5:30 p.m., Monday through Friday, except on public holidays.

(1) Provide information sufficient to identify the record, e.g., the individual's own name, the name of the record, and decision number, date and place of birth, etc.;

(2) Provide identification sufficient to verify the individual's identity, e.g., driver's license, passport, identification or Medicare card; and

(3) Any individual requesting access to records or information pertaining to himself or herself may be accompanied by a person of the individual's own choosing while reviewing the records or information. If an individual elects to be so accompanied, advance notification of the request will be required along with a written statement authorizing disclosure and discussion of the record in the presence of the accompanying person at any time, including the time access is granted.

(c) Any individual making a request for access to records or information pertaining to himself or herself by mail must address the request to the Administrative Officer (Privacy Officer), Claims Settlement Commission, 600 E Street, NW., Room 6002, Washington, DC 20576, and must provide information acceptable to the Administrative Officer to verify the individual's identity.

(d) Responses to requests under this section normally will be made within ten (10) days of receipt (excluding Saturdays, Sundays, and legal holidays). If it is not possible to respond to requests within that period, an acknowledgment will be sent to the individual within ten days of receipt of the request (excluding Saturdays, Sundays, and legal holidays).

§ 503.6 Determination of requests for access to records.

(a) Upon request made in accordance with § 503.5, the Administrative Officer will:

(1) Determine whether or not the request will be granted;

(2) Make that determination and provide notification within a reasonable period of time after receipt of the request.

(b) If access to a record is denied because information has been compiled by the Commission in reasonable anticipation of a civil or criminal action or proceeding, the Administrative Officer will notify the individual of that determination and the reason therefor.

(c) If access to the record is granted, the individual making the request must notify the Administrative Officer whether the record requested is to be copied and mailed to the individual.

(d) If a record is to be made available for personal inspection, the individual must arrange

the Administrative Officer a mutually agreeable time and place for inspection of the record.

§ 503.7 Amendment of a record.

(a) Any individual may request amendment of a record pertaining to himself or herself according to the procedure in paragraph (b) of this section, except in the case of record described under paragraph (d) of this section.

(b) After inspection by an individual of a record pertaining to himself or herself, the individual may file a written request, presented in person or by mail, with the Administrative Office for amendment to a record. The request must specify the particular portions of the record to be amended, the desired amendments and the reasons therefor.

(c) Not later than ten (10) days (excluding Saturdays, Sundays, and legal holidays) after receipt of a request made in accordance with this section to amend a record in whole or in part, the Administrative Officer will:

(1) Make any correction of any portion of the record which the individual believes is not accurate, relevant, timely or complete and thereafter inform the individual of such correction;

(2) Inform the individual, by certified mail return receipt requested, of the refusal to amend the record, setting forth the reasons therefor, and notify the individual of the right to appeal the determination as provided under Sec. 503.8 of this part.

(d) The provisions for amending records do not apply to evidence presented in the court or Commission proceedings in the adjudication of claims, nor do they permit collateral attack upon what has already been subject to final agency action in the adjudication of claims programs previously completed by the Commission pursuant to statutory time limitations.

§ 503.8 Appeals from denial of requests for amendment to records.

(a) An individual whose request for amendment of a record pertaining to the individual is denied may request a review of that determination. The request must be addressed to the Chair of the Commission, and must specify the reasons for which the refusal to amend the record is challenged.

(b) If on appeal the refusal to amend the record is upheld, the Commission will permit the individual to request amendment of the record.

individual to file a statement setting forth the reasons for disagreement with the determination. The statement must also be submitted within 30 days of receipt of the denial. The statement will be included in the system of records in which the disputed record is maintained and marked so as to indicate:

- (1) That a statement of disagreement has been filed, and
- (2) Where in the system of records the statement may be found.

§ 503.9 Fees.

Fees to be charged, if any, to any individual for making copies of that individual's record excluding the cost of any search for and review of the record will be as follows:

- (a) Photocopy reproductions: each copy \$0.15.
- (b) Where the Commission undertakes to perform for a requester, or any other person, services which are clearly not required to be performed under the Privacy Act, either voluntarily or because those services are required by some other law, the question of charging fees for those services will be determined by the official or designee authorized to release the information under the Federal user charge statute, 31 U.S.C. 583a, any other applicable law, and the provisions of § 502.13 of part 502 of this chapter.

§ 503.10 Exemptions.

No system of records maintained by the Foreign Claims Settlement Commission is exempt from the provisions of 5 U.S.C. 552a as permitted under certain conditions by 5 U.S.C. 552a(k). However, the Chair of the Commission reserves the right to promulgate rules in accordance with the requirements of 5 U.S.C. 553(b)(1), (2) and (3), and 5 U.S.C. 553(c) and (e) to any system of records maintained by the Commission in accordance with the provisions of 5 U.S.C. 552a(k).

§ 503.11 Reports.

- (a) The Administrative Officer or designee will provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any Commission system of records, as required by 5 U.S.C. 552a(o).

(b) If at any time a system of records maintained by the Commission is determined to be exempt from the application of 5 U.S.C. 552a in accordance with the provisions of 5 U.S.C. 552a(j) and (k), the number of records contained in such system will be separately listed and reported to the Office of Management and Budget.

§ 503.12 Notices.

The Commission will publish in the *Federal Register* at least annually a notice of the existence and character of the systems of records which it maintains. Such notice will include:

- (a) The name and location of each system;
- (b) The categories of individuals on whom the records are maintained in each system;
- (c) The categories of records maintained in each system;
- (d) Each routine use of the records contained in each system including the categories of records and the purpose of each use;
- (e) The policies and practices of the Commission regarding storage, retrievability, access controls, retention, and disposal of the records;
- (f) The title and business address of the agency official who is responsible for each system of records;
- (g) Commission procedures whereby an individual can be notified if a system of records contains a record pertaining to that individual;
- (h) Commission procedures whereby an individual can be notified how to gain access to a record pertaining to that individual contained in a system of records, and how to contest the content, and
- (i) The categories of sources of records in each system.

[\[TOP\]](#)

Title 48—Federal Acquisition Regulations System

Chapter 28—Department of Justice

PART 2824—PROTECTION OF PRIVACY AND FREEDOM OF INFORMATION

Subpart 2824.2—Freedom of Information Act

Sec.

2824.202 Policy.

Authority: 28 U.S.C. 510; 40 U.S.C. 486(c); 28 CFR 0.75(j) and 28 CFR 0.76(j).

Source: 63 FR 16130, Apr. 2, 1998, unless otherwise noted.

Subpart 2824.2—Freedom of Information Act

2824.202 Policy.

Procedures for processing Freedom of Information Act requests are set forth in Department regulations and 28 CFR part 16.

[63 FR 16130, Apr. 2, 1998]

[\[TOP\]](#)



Website Developed by: GPO, Digital Media Services (DMS)