

# FBI INFORMATION SHARING REPORT

2011





## Table of Contents

<b>I. EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>II. RECENT HIGHLIGHTS.....</b>	<b>3</b>
<b>III. OPTIMIZING INFORMATION SHARING WITH PARTNERS TO ENABLE DECISION ADVANTAGE .....</b>	<b>4</b>
<b>UNDERSTANDING NEEDS .....</b>	<b>4</b>
OPERATIONAL COORDINATION.....	4
MUTUAL UNDERSTANDING THROUGH ENGAGEMENT.....	4
INTERAGENCY THREAT ASSESSMENT AND COORDINATION GROUP .....	4
STANDARDIZATION .....	5
FORMAL DOCUMENTATION OF INFORMATION NEEDS FROM STATE AND LOCAL FUSION CENTERS.....	5
<b>MANAGING RELATIONSHIPS .....</b>	<b>5</b>
CHANGES WITHIN FBI .....	5
NATIONAL JOINT TERRORISM TASK FORCE AND JOINT TERRORISM TASK FORCES.....	5
NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE .....	6
CRIMINAL JUSTICE INFORMATION SERVICES (CJIS).....	6
STATE AND LOCAL FUSION CENTERS .....	7
TRIBAL AND BORDER COMMUNITIES.....	9
DRUGS, GANGS, AND OTHER CRIMES.....	9
LAW ENFORCEMENT GENERALLY.....	10
BETTER SHARING THROUGH IMPROVED MARKING GUIDANCE.....	11
<b>LEVERAGING CAPABILITIES OF PARTNERS .....</b>	<b>11</b>
TERRORIST WATCHLISTING AND SCREENING COMMUNITIES.....	11
BIOMETRICS.....	11
PRIVATE SECTOR STAKEHOLDERS.....	12
SHARING WITH INTERNATIONAL PARTNERS.....	13
<b>IV. MAXIMIZING AND INTEGRATING INFORMATION SHARING CAPABILITIES.....</b>	<b>14</b>
<b>DISCOVER, ACCESS, AND EXPLOIT INFORMATION BASED ON MISSION NEED.....</b>	<b>14</b>
LAW ENFORCEMENT ONLINE.....	14
LAW ENFORCEMENT NATIONAL DATA EXCHANGE.....	15
DATA INTEGRATION AND VISUALIZATION SYSTEM (DIVS).....	17
NEXT GENERATION IDENTIFICATION SYSTEM.....	17
<b>ENHANCE CAPABILITIES FOR COLLABORATION AND INFORMATION SHARING .....</b>	<b>18</b>
THE BIOMETRIC CENTER OF EXCELLENCE .....	18
THE eGUARDIAN SYSTEM AND SUSPICIOUS ACTIVITY REPORTING .....	19
TERRORIST SCREENING CENTER (TSC).....	20

<b><u>V. MAXIMIZING AND INTEGRATING CAPABILITIES TO SECURE INFORMATION .....</u></b>	<b><u>22</u></b>
IDENTITY MANAGEMENT .....	22
USER AUTHORIZATION AND ACCESS.....	23
AUDIT AND MONITORING .....	24
<b><u>VI. STRENGTHENING THE GOVERNANCE FRAMEWORK .....</u></b>	<b><u>24</u></b>
<b>FBI GOVERNANCE OF INFORMATION SHARING .....</b>	<b>25</b>
INFORMATION SHARING POLICY BOARD. ....	25
ACCESS POLICY GROUP.....	26
INFORMATION SHARING TEAMS. ....	26
CHIEF INFORMATION SHARING OFFICER. ....	26
<b>INTERAGENCY GOVERNANCE .....</b>	<b>27</b>
INFORMATION SHARING AND ACCESS INTERAGENCY POLICY COMMITTEE. ....	28
OFFICE OF THE PROGRAM MANAGER FOR THE INFORMATION SHARING ENVIRONMENT. ....	29
INTELLIGENCE COMMUNITY INFORMATION SHARING STEERING COMMITTEE. ....	29
<b><u>VII. PROMOTING A CULTURE OF RESPONSIBLE INFORMATION SHARING .....</u></b>	<b><u>29</u></b>
INCORPORATING INFORMATION SHARING .....	29
ENSURING ACCOUNTABILITY .....	30
TRAINING AND AWARENESS.....	30
AWARDS.....	31
<b><u>APPENDIX B: DESCRIPTION OF FBI FINISHED INTELLIGENCE PRODUCTS.....</u></b>	<b><u>37</u></b>
<b><u>APPENDIX C: ACRONYMS .....</u></b>	<b><u>40</u></b>

## I. EXECUTIVE SUMMARY

*Since September 11, 2001, the FBI has shifted from a traditional crime-fighting agency into an intelligence-led, threat-driven organization, guided by clear operational strategies. Today's FBI is focused on predicting and preventing the threats we face while at the same time engaging with the communities we serve. This shift has led to a greater reliance on technology, collaboration, and information sharing.<sup>1</sup>*

Effective information exchange is a requisite for the success of the unique Federal Bureau of Investigation (FBI) national security and law enforcement missions. Dynamic operations, a shifting policy environment, and improvements in technological capabilities characterized the FBI in 2011, reinforcing continued need for broad, agile, but secure information exchange. The FBI is committed to sharing timely, relevant, and actionable intelligence with the widest appropriate audience while protecting the privacy and civil liberties of the American people. It is also committed to making the best possible use of information these partners share with the FBI. The FBI continually promotes an information-sharing culture, deploys new technologies, and refines its policies and procedures in support of its commitment.

Strategic integration of technology increased FBI capacity to discover, access, share, and exploit information. Technology and policy enabled continued efforts to safeguard information, improve oversight, and protect against external and insider threats.

Activities in 2011 reinforced the concept that policy and governance are critical to information safeguarding and secure sharing. The National Security Staff (NSS) sponsored new efforts among the Executive Departments to enhance information sharing. The Office of the Director of National Intelligence (ODNI) established the ground rules for the sharing of sensitive intelligence among the members of the Intelligence Community (IC), including the FBI. The Department of Justice assumed new roles and continues to sponsor other initiatives that enhance FBI information sharing. Within the FBI, the Information Sharing Policy Board (ISPB) provided senior-level policy oversight, while the Chief Information Sharing Officer coordinated information sharing policy issues and implementation of both FBI and external mandates.

In 2011 the FBI continued to promote a culture of responsible sharing through several initiatives interwoven into daily operations. This was demonstrated in how the FBI, in coordination with its partners, dealt with threat information specifically related to the tenth anniversary of 9/11.

The FBI participated in several significant information sharing initiatives in 2011 and continues to promote appropriate sharing and collaboration. The FBI remains committed to ensuring that information sharing practices are an integral part of the FBI culture and advance its mission: to protect the United States and defeat national security threats while preserving the privacy and civil liberties of our citizens. This report, presented by the FBI Chief Information Sharing Officer (CISO), summarizes and characterizes the many information sharing activities currently

<sup>1</sup> Robert A. McFeely, Special Agent in Charge, Baltimore Office, Federal Bureau of Investigation. Statement before the Senate Judiciary Committee (Wilmington, Delaware; June 20, 2011). <http://www.fbi.gov/news/testimony/information-sharing-efforts-with-partners-span-many-fbi-programs>

engaged in by the FBI. The report is presented in a slightly different manner this year, to acknowledge the many collaborations and information sharing initiatives and activities in which the FBI participates throughout the diverse information sharing environment.

The need for information sharing will endure as the complexity of the national security threat environment demands situational awareness and participation by partners across the spectrum. This Information Sharing Report highlights the efforts undertaken by FBI to ensure law enforcement remains relevant to this process in a manner consistent with national security and applicable legal standards relating to privacy and civil liberties.

## II. RECENT HIGHLIGHTS

Our nation's security requires classified information to be shared effectively with authorized users around the world, but also requires sophisticated and vigilant means to ensure it is shared securely. Investigations into the 2010 WikiLeaks disclosures exposed the need for systemic oversight of policy compliance. Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," resulted from an intensive year long security review by White House and National Security officials, including the FBI. The team that drafted this executive order sought to find a proper balance between security and the need for agencies to share classified information, one of weaknesses revealed by the Sept. 11, 2001 terrorist attacks. President Obama's signature on the Executive Order (EO) on October 7, 2011 codified many steps initiated or reinforced in the year since large volumes of classified documents were made public on the internet via the WikiLeaks website.

The EO affirmed that agencies bear the primary responsibility for meeting the twin goals of responsible sharing and safeguarding of classified information on computer networks consistent with appropriate protections for privacy and civil liberties. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards apply to all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.

Under the Order, the government created a Senior Information Sharing and Safeguarding Steering Committee, chaired by senior Office of Management and Budget (OMB) and National Security Staff (NSS) representatives, to coordinate information sharing and to ensure that agencies that use classified computer networks protect information. The FBI is represented in this committee by the Associate Executive Assistant Director of the Information Technology Branch and the Chief Information Sharing Officer. Under the oversight of the FBI Director's Office, they helped institute a variety of measures to improve the Nation's posture against identified vulnerabilities. These safety measures included many initiatives that were already underway within the FBI, such as: enhancing control of removable media; improved identity management, including reducing user anonymity and increasing user attribution across classified networks, in a manner applicable to multiple federal agencies; and bringing advanced technologies to bear against insider threats, and on security and access controls.

Many of the initiatives and programs highlighted in other sections of this report were directly impacted by these activities. The FBI continues to play important roles in investigations into unauthorized disclosures, development of mitigation activities against insider threat, and in developing appropriate governance and policy to ensure appropriate level of oversight under the new EO.

### **III. OPTIMIZING INFORMATION SHARING WITH PARTNERS TO ENABLE DECISION ADVANTAGE**

Information shared among trusted partners drives national security and law enforcement. The FBI understands the value of collaboration with its partners in maintaining security, and remains committed to strengthening ties at all levels, from local to international. The FBI National Information Sharing Strategy (NISS) provides the common vision, goals, and framework needed to guide information sharing initiatives with federal, state, local, and tribal agency partners, foreign government counterparts, and private sector stakeholders. Through enhanced understanding of their diverse needs, the FBI is able not only to improve information acquisition but leverage partner capabilities to mitigate threats to people and infrastructure.

#### **Understanding Needs**

The FBI uses a variety of mechanisms to ensure that it understands the information needs of its partners and shares its own needs with these partners.

**Operational coordination.** The ongoing efforts of the FBI's Joint Terrorism Task Forces (JTTFs), and embedded Terrorism Liaison Officers (TLOs) ensure that intelligence and information needs are well understood for operational purposes.

**Mutual understanding through engagement.** Regular liaison and engagement through nationwide efforts, FBI Field Offices, Field Intelligence Groups (FIGs), Regional Intelligence Groups (RIGs), other liaison and attaché roles, and outreach programs such as the Domestic Security Alliance Council (DSAC) and the Department of State's Overseas Security Alliance Council (OSAC), ensure that the FBI is able to observe and absorb the information needs of its partners. Informal contact at international, national and regional conferences and symposia also serve as mechanisms to improve understanding of information requirements.

**Interagency Threat Assessment and Coordination Group.** The Interagency Threat Assessment and Coordination Group (ITACG) is charged with providing advice to IC agencies on how to tailor their products to satisfy the needs of state, local, tribal, territorial, and private sector entities so that they, in turn, can better serve their customers. Detailees from outside the federal government assigned to the ITACG worked with FBI Headquarters personnel to ensure law enforcement/first responder needs were understood by the national counterterrorism community and represented in intelligence production. Some issues addressed through this relationship in 2011 included updates to ITACG Standard Operating Procedures, production of Roll Call Release and other analytic products, and guides for public safety personnel to correspond with a second, updated edition of their *Intelligence Guide for First Responders*.

Senior executives at the FBI, including the ISPB, also received visits and briefings from ITACG members on several occasions during the year. In addition to ensuring FBI senior executives are aware of the ITACG activities; this direct interaction with FBI senior leaders keeps the ITACG members informed of activities and ways in which the FBI shares information throughout the national community.

**Standardization.** Improvement in intelligence collection, analysis, and reporting can also be achieved through better information gathering and matching intelligence against requirements. Internally, the FBI has incorporated upgraded technology to increase standardization, and make collecting and sorting intelligence easier for intelligence analysts. These updates facilitate better interoperability between system applications for the intelligence collection and analysis communities within FBI.

**Formal documentation of information needs from State and Local Fusion Centers.** The FBI's Directorate of Intelligence (DI) reviews and updates collection requirements on a regular basis. The DI and the Chief Information Sharing Officer partnered with the US Department of Homeland Security (DHS) Intelligence and Analysis Directorate, the Program Manager-Information Sharing Environment (PM-ISE), and ITACG, to conduct a formal study regarding fusion center information needs. Under the aegis of the Assured Secret Network Interoperability Working Group of the Information Sharing and Access Interagency Policy Committee (ISA IPC), the group documented, validated, and prioritized information requirements at the state and local levels. This established foundational requirements needed to inform development of technical connectivity and access to sensitive information for fusion centers. The study revealed large overlap between FBI and State, local, tribal law enforcement needs. Documenting these needs ensured that validated information needs were communicated to federal partners, informing overall information sharing activities. The study was a topic of discussion at the 2011 National Fusion Center Conference and special-topic meetings during the conference. The results of this study were briefed to the Fusion Center Subcommittee of the ISA IPC and were incorporated into work being conducted within DHS.

## **Managing Relationships**

The law enforcement and national security missions are dependent upon cooperation and collaboration between multiple organizations for information acquisition, exploitation, and transformation to actionable intelligence. Information sharing relationships exist at all levels of government, from local to international. Organizations at each level work within and between communities to maintain public safety and provide for common defense.

**Changes within FBI.** In 2011 a new DI Branch, the Intelligence Integration Branch (IIB), was created to enhance sharing and outreach efforts. The IIB is specifically charged with engaging federal, state, local, tribal, and IC partners to increase the effectiveness of information sharing and also to coordinate efforts to combat violent extremism.

The IIB worked with other elements of the DI and the Department of Justice as well as the Office of the Director of National Intelligence Partner Engagement Division, to ensure law enforcement needs were represented in IC activities and analytic efforts.

**National Joint Terrorism Task Force and Joint Terrorism Task Forces.** The FBI-led National Joint Terrorism Task Force (NJTTF) is a multi-agency task force consisting of 48 government agencies and critical industry representatives collocated at the National Counter Terrorism Center (NCTC). The mission of the NJTTF is twofold: 1) to enhance communications, coordination and cooperation concerning terrorism intelligence among federal,

state, local, and tribal government agencies representing the intelligence, law enforcement, defense, diplomatic, public safety and homeland security communities; and 2) to support the JTTFs throughout the United States.

Located in more than 100 cities across the United States — including one in each of the FBI's 56 field locations — JTTFs comprise small teams of highly-trained, locally-based investigators, analysts, linguists, Special Weapons And Tactics (SWAT) experts, and other specialists from dozens of federal, state, local, and tribal law enforcement organizations and federal intelligence agencies. JTTFs investigate leads, gather evidence, make arrests, provide security for special events, conduct training, collect and share intelligence, and respond to threats and incidents at a moment's notice.

The JTTFs work across organizational boundaries on national terrorism issues. JTTFs, however, have a strict counterterrorism focus in contrast to state and local fusion centers' broader focus, and JTTFs actually conduct investigations as well as carrying out the "fusion" function of gathering information from multiple investigations to support analysis and situation awareness.

**Nationwide Suspicious Activity Reporting Initiative.** The FBI actively worked throughout the year to ensure that state, local, and tribal law enforcement agencies are aware of specific types of suspicious activities related to terrorism that they should report, and the process through which they should report this information. The FBI's unclassified eGuardian system is available to any law enforcement agency as a means to share Suspicious Activity Reports (SARs). This web-based system enables law enforcement agencies to input their own reports and run searches against other SARs. As a full participant in the Nationwide Suspicious Activity Reporting Initiative (NSI), the FBI and its eGuardian system serve as a means to enhance the reporting and sharing of terrorism-related suspicious activity reports. The FBI ensures that indicators developed and vetted through the NSI are highlighted for state, local and tribal law enforcement agency access. Threat information assessments, unclassified reports received through the classified Guardian system, and other analyses are posted on the eGuardian site to facilitate broader FBI sharing directly with the law enforcement agencies that participate in eGuardian.

The FBI is working with the NSI to enhance sensitive but unclassified information sharing among all mission partners in order to protect the security of the homeland. This initiative helps formalize the sharing of information currently taking place between state, local, and tribal partners, and leverages the already successful relationships between state, local, and territorial law enforcement partners and the FBI's JTTFs.

In mid-2011, the FBI began regularly producing SAR products for use by DHS components, the IC, law enforcement agencies, and the private sector. Products range from stand-alone documents addressing suspicious activities or summarizing reporting, to routine all-source analytic products that incorporate SAR data. In 2011 the FBI posted over 900 intelligence products on the Law Enforcement Online (LEO) site for authorized LE partners. In addition, the FBI produced 48 Joint Intelligence Bulletins with DHS.

**Criminal Justice Information Services (CJIS).** The FBI's CJIS Division has significantly furthered information sharing, not only with continuing efforts like LEO, the National Crime

Information Center (NCIC), and the National Data Exchange (N-DEX), but notably with major developments in biometrics, and in particular the Biometric Center of Excellence. All of these will be referenced later in this report.

**State and Local Fusion Centers.** Fusion centers have become an established mechanism for communication and coordination of threat information domestically. In 2011, the FBI and the DHS ensured that fusion centers remained an important focal point for coordination of their joint information sharing efforts and ensuring they met the needs of state, local, and tribal law enforcement. While the development of the fusion center network is progressing rapidly and developing into a coordinated enterprise, it is not yet a seamless web which connects to all state, local, and tribal law enforcement agencies. Local control over the form and development of the fusion centers necessarily creates differences in the focus, maturity, capabilities, and comprehensiveness of outreach of the fusion centers.

Successful engagement between the FBI and fusion centers is dependent upon the seamless integration and coordination of information sharing between FBI Field Offices, their FIGs, and the Fusion Centers. The FBI recognizes that a “one size fits all” approach to engagement is not practical based upon the variability and maturity among fusion centers. However, the FBI has implemented a standardized approach to characterize relationships and types of engagement to promote consistency in language, and to help increase understanding of the types of partnerships the Bureau maintains on a nationwide basis.

In August 2011, the Executive Assistant Director of the National Security Branch approved the FBI’s engagement plan with fusion centers. In addition to providing national level support to fusion centers with respect to achieving DHS-mandated Baseline Capabilities, and committing resources in accordance with the National Fusion Center Sub-Committee’s Resource Allocation Criteria, the FBI provides policy and governance at the field level based on the following guiding principles:

- The JTTFs will remain the principal operational-level coordination organizations, and they will interact with all affiliated partners, to include those involved with fusion centers.
- Field offices will consistently coordinate with fusion centers for the best suited alignment with the FBI’s mission, with added emphasis on shared counterterrorism missions. The Baseline Capabilities (Management and Administrative Capabilities, Management/Governance, Mission Statement) state that fusion centers adopting an all-crimes approach should “*liaise with applicable agency and multijurisdictional task forces and intelligence units,*” which should include JTTFs and Field Intelligence Groups.
- Field offices will emphasize the importance of representation by ensuring FBI Executive Management’s participation on the Fusion Center Governance Board/Advisory Council.
- It is understood that fusion centers will operate in an accredited, secure space, and be capable of receiving, analyzing, disseminating, and gathering/collecting information that contributes to the current threat environment. The secure work environment includes the physical infrastructure and the IT infrastructure that is required by FBI personnel to share information at all levels of classification across multiple programs as well as with the Intelligence Community and local and state partners.

- It is critical that fusion centers understand the importance of immediately sharing emerging, terrorism-related information with the FBI.

Field offices will determine whether the fusion center(s) within their Area of Responsibility (AoR) support these principles. The FBI will collectively work with those fusion centers to employ the following actions:

- As resources become available, field offices will designate at least one full-time, experienced Intelligence Analyst (IA) to fusion centers meeting the above criteria.
- The FBI will continue to fund FBINet (Secret-level) connectivity in fusion centers that meet mandatory security requirements.
- At the corporate level, the FBI, in collaboration with DHS, will regularly assess fusion centers to determine their compliance with the *Fusion Center Guidelines and the Baseline Capabilities*. In addition, FBI Program Managers will assess FBI engagement with fusion centers in accordance with the principles set forth above.

### **Governance and Coordination of fusion center engagement.**

In coordination with the Office of General Counsel, the FBI created a standardized Memorandum of Understanding (MOU) for FBI participation in Fusion Centers that will be executed by the field office Special Agent in Charge and the State Governor or designee. Mirroring the success of the standardized JTTF MOU and interagency cooperation, the fusion center MOU will address the principles and initiatives while being mindful of privacy and civil liberties.

The FBI's DI and the Training Division recently posted numerous training modules on the unclassified Virtual Academy site for access by non-FBI, fusion center, and law enforcement partner agency personnel. The catalog of courses is vast, and includes topics ranging from basic computer skills to intelligence to investigative program topics. Examples of courses in the current catalogue include: Information Awareness; Introduction to Collection Management; Privacy: It's Every Employee's Business; Government Ethics, Information Security and the Internet; Organizational Scope of Critical Thinking; and N-DEx System Overview.

In December 2011, the FBI's DI implemented an orientation program in Washington, DC for fusion center Directors and FBI field office Executive Managers. The format was a one-day round table conference at FBI Headquarters during which field office management, fusion center Directors, DI executives and personnel participated in mission briefs, open discussion and exchange of ideas. This program will strengthen relationships by providing fusion center Directors with a detailed overview of FBI information sharing, as well as operational and intelligence processes.

In addition, the FBI's DI has also played an integral role in creating a newsletter intended to reach the general law enforcement community. This newsletter will provide intelligence information from both a global and local perspective. Initial publication of this newsletter is scheduled for the first quarter of 2012.

FBI expenditures in support of fusion centers in Fiscal Year 2011 were approximately \$917,000. The FBI currently has 96 full-time and part-time personnel assigned to 55 state, local, tribal, and territorial fusion centers, and has established operational access to FBINet in 47 of the 72 centers. The role of the embedded personnel is to increase responsible information sharing through efforts to enhance the understanding and knowledge of both local and FBI needs, and to facilitate appropriate access to FBI systems. Embedded staff members also work to leverage the information collection capabilities of the fusion centers to support FBI mission needs and to utilize the fusion centers and dissemination points for FBI intelligence products, such as Intelligence Assessments, Intelligence Bulletins, and Intelligence Information Reports.

**Tribal and Border Communities.** Tribal governments and law enforcement agencies continued to work with the FBI to counter crime through participation in joint investigative efforts, liaison programs, and initiatives like the FBI-lead Safe Trails Task Force (STTF). The STTF unites federal, state, local, and tribal law enforcement agencies to combat crime and enhance information sharing practices in Indian Country. There are 19 active STTFs. The FBI also has over 100 Special Agents working in support of Indian Country investigations.

The FBI has multiple other avenues of outreach to state, local, and tribal agencies, including those along the northern and southern borders. These include the Joint Terrorism Task Forces, formal liaison programs, LEO, eGuardian and Field Intelligence Groups. The FBI's participation and leadership in multi-agency operations such as the Terrorist Screening Center, National Counterterrorism Center, Interagency Threat Assessment Coordination Group (ITACG), High Intensity Drug Trafficking Areas Program (HIDTAs), Organized Crime Drug Enforcement Task Forces, El Paso Intelligence Center, Port Area Maritime Security Committees, and Joint Interagency Drug Task Forces also provide a great venue for outreach with local and tribal agencies.

The best interaction, though, often comes through informal contacts and establishment of ongoing relationships between agents and analysts in the field with federal, state, local and tribal counterparts. Activities that support non-counterterrorism focus mission areas generate information highly relevant to border issues. This information flows through networks connected to those issues – including through FBI border liaison agents, RIGs, and other FBI networks. Since not all local agencies have the ability to communicate via secure electronic means, face-to-face meetings and telecommunications between trusted partners are critical. This is especially true with respect to the tribal areas and with border issues. FBI also participates in ad hoc working groups throughout the nation (as well as on the borders) that develop information relevant to border issues. For instance, information developed regarding gangs and criminal networks frequently intersect with human smuggling or other border community issues. This information will flow through appropriate law enforcement channels.

**Drugs, Gangs, and other Crimes.** The FBI continued to lead and work in task forces and operation centers with law enforcement and other agencies from all levels of government to cooperatively assimilate information and tackle the often inter-related crimes linked to drug trafficking, gangs, corruption, and violent crimes including terrorism.

The FBI collaborated with High Intensity Drug Trafficking Area (HIDTA) partners to formalize information requirements and processes, and to incorporate them into a national threat information network. Like the FBI, HIDTAs are finding that information developed through their traditional operational roles increasingly overlaps with information developed in support of national security concerns. Discipline in exercising responsibilities and clear communication are among the best practices law enforcement entities shared during meetings over 2011.

The FBI continued its relationship with the National Gang Intelligence Center (NGIC), which shares information and analysis on the growth, migration, and association of gangs that threaten communities throughout the United States. The NGIC manages the exchange of gang information through LEO, the National Crime Information Center (NCIC), the Violent Gang and Terrorist Organizations File (VGTOF), GangNet, and other major systems. NGIC supports law enforcement requests for information on suspected or known gangs and gang members, and consolidates gang-related investigative data and raw intelligence into an up-to-date library of gang identification symbols, clothing, signs, tattoos, codes, writings, graffiti, and philosophies. Over 170,000 NGIC files are available to state, local, and tribal law enforcement partners.

Sponsored by the Department of Justice, the Organized Crime and Drug Enforcement Task Force (OCDETF) Fusion Center (OFC) aggregates the resources of multiple agencies and actively uses intelligence to disrupt and dismantle the most significant drug trafficking and money laundering enterprises. OFC participants include DOJ components (FBI, ATF, and DEA, whose personnel represent the largest single segment of the OFC workforce) and other agencies, such as the Internal Revenue Service, the US Postal Service, and the US Coast Guard. In total, 15 agencies are represented at OFC, with additional agencies expected to join the network.

The FBI ensured that the needs of the OFC are incorporated into the design of Sentinel, the FBI's new case management system. FBI shares with OFC partner agencies data from FBI automated case files related to OCDETF, gang and other criminal enterprise matters, Controlled Substances Act/drug-related offenses, Firearms Act offenses, kidnapping, violent crimes, Indian Country criminal activity on a government reservation, health care fraud, and confidential human source reporting in drug and general crimes matters, and extortion. The FBI screens case file data using automated and manual reviews prior to transmittal. Documents are provided on a regular basis. The FBI also provides more than 30 personnel in support of the OFC, including Supervisory Special Agents, Intelligence Analysts, and Management and Program Analysts

**Law enforcement generally.** The FBI has engaged with the law enforcement community for many decades, and since 2001 these continuing relationships have been leveraged to support national security issues as well. One such way is through participation in the Criminal Intelligence Coordinating Council (CICC), a working group under the DOJ Global Advisory Committee that makes policy recommendations to help agencies establish criminal intelligence sharing policies, procedures, standards, technologies, and training. The CICC comprises representatives from law enforcement and homeland security agencies from all levels of government. The CICC acts as an advocate for state, local, and tribal law enforcement organizations, and their efforts to develop and share criminal intelligence in the promotion of public safety and national security. Senior leaders from FBI regularly make presentations to and participate in the CICC forums and other law enforcement-related organizations such as the

International Chiefs of Police (IACP), the National Sheriffs Association, Major Cities Chiefs Association, and the National Academy for Law Enforcement.

**Better sharing through improved marking guidance.** The FBI Security Division supported DI efforts through review and clarification of internal security and classification marking policy. The FBI's "official use only" Policy guidance published in May 2011 described in detail how to mark and share law enforcement sensitive information with non-law enforcement domestic and international partners.

### **Leveraging Capabilities of Partners**

The FBI relies on the inherent capabilities of mission partners in several different communities to gather and share information in support of common missions. Through continued engagement, the FBI seeks not only to improve information acquisition but leverage partner capabilities to mitigate threats to people and infrastructure.

**Terrorist Watchlisting and Screening Communities.** The FBI provides a strong leadership role in the Watchlisting and Screening Community, notably through its management of the Terrorist Screening Center (TSC), as well as through representation in various national level policy, law enforcement, and intelligence committees. Relationships developed through these roles and decades of investigations are critical to ensuring continued open dialogue, business process and information sharing enhancements among the partners. Due to trust and standardized managed processes, for instance, law enforcement encounter data is now being provided to counterterrorism analysts and processed daily in a secure manner for sharing with the broader IC. The FBI's role in several related efforts in law enforcement mean that technology or techniques developed in one arena can be readily recognized as applicable for the IC and counterterrorism analysis.

**Biometrics.** Combining the search power of the FBI's biometric identification systems with the biometric databases of local, state, national, and international partners enables more comprehensive use of key resources to identify criminals and terrorists. At the CJIS Division, advances in biometric interoperability have been developed through continued information sharing between the FBI, the Department of Homeland Security (DHS), the Department of State (DOS), and the Department of Defense (DOD). This partnership has provided FBI increased access to DHS's Automated Biometric Identification System (IDENT) and the DOD's Automated Biometric Identification System (ABIS), enabling successful identification and exchange of information on criminals who might otherwise have been missed. These technology advances have also incorporated capabilities to ensure that the privacy and civil liberties of the American people are protected.

Through CJIS interoperability initiatives, the FBI and other government agencies can more effectively and efficiently exercise national security responsibilities.

- The search of the full DHS IDENT repository is now available to additional noncriminal justice agencies and programs that use mobile devices to gather biometric information at the scene of an incident or investigation and check it against the FBI's partner databases. Searches are taking place in over 80 percent of the states and in one US territory.

- The CJIS staff teamed with DHS's Immigration and Customs Enforcement (ICE) agency to successfully submit fingerprints and receive responses from the IDENT, the ABIS, and the IAFIS via mobile devices. At least 80 agencies are taking part in the ICE's international Biometric Identification Transnational Migration Alert Program.
- The DHS Customs and Border Protection personnel can use a rapid response capability to access the full IAFIS Criminal Master File at four major airport inspection locations.
- The Coast Guard can check crew lists against the ICE Biometric Identification Transnational Migration Alert Program forwarded through ABIS to IAFIS.

**Private Sector Stakeholders.** The FBI is committed to developing effective and efficient information sharing partnerships with the private sector. While ensuring that all proprietary information is protected, the FBI will share information on incidents, threats, consequences and vulnerabilities, as appropriate. Each operational program (Counterintelligence, Counterterrorism, Criminal, Cyber, and Weapons of Mass Destruction) and Community Outreach has an organized, ongoing effort to engage with the private sector, and to increase awareness and build partnerships. FBI leverages capabilities of these partners through programs like TRIPWIRE and community outreach programs.

InfraGard is a partnership between the FBI, state and local law enforcement agencies, academic institutions, an association of businesses, and other organizations dedicated to protecting the United States national critical infrastructure by sharing information regarding both cyber and physical threats and vulnerabilities. The goal of InfraGard is to promote an ongoing dialogue and timely communication between InfraGard members and the FBI for investigative and intelligence gathering purposes. Since its founding in 1996, InfraGard has helped to establish a relationship of trust and credibility between the private sector and the FBI regarding the exchange of terrorism, intelligence, criminal, and security information.

The FBI provides information to InfraGard members in the form of alerts and advisories via secure email and a secure website. InfraGard members share information with the FBI and with each other by posting articles on the secure website, communicating via secure e-mail, bulletin boards, list servers, and networking at membership meetings. InfraGard chapters are geographically linked with FBI field office territories, and are assigned an FBI Special Agent Coordinator. The FBI Coordinator also works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters.

The Domestic Security Alliance Council (DSAC), a strategic partnership between the FBI and the US private sector, was established to promote the timely and effective exchange of information. DSAC advances the FBI mission of preventing, detecting, and investigating criminal acts, particularly those affecting interstate commerce, while advancing the ability of the US private sector to protect its employees, assets, and proprietary information.

The Cyber Initiative Resource Fusion Unit (CIRFU) is an FBI Cyber Division unit embedded at the National Cyber Forensics and Training Alliance (NCTFA), a non-profit corporation located in Pittsburgh, Pennsylvania. The NCTFA is a fusion center combining personnel, resources and law enforcement expertise with academia and the private sector. Experts from federal agencies, universities, Internet security companies, Internet service providers, the telecommunications

sector, and the financial sector share information and collaborate on security breaches, as well as identifying current and emerging cyber threats.

The Counterintelligence Strategic Partnership Unit and the Strategic Partnership Coordinator in each FBI Field Office collaborate with the key private sector stakeholders of critical technology targeted by foreign adversaries. This is accomplished by fostering communication and building awareness with key academic, business and strategic entities, and by educating and enabling our partners to identify what is at counterintelligence risk and how to protect it. The FBI calls this “knowing your domain:” identifying the research, information and technologies that are targeted by our adversaries, and establishing an ongoing dialog and information exchange between partners to change behaviors and reduce opportunities that benefit the opposition.

**Sharing with International Partners.** The FBI routinely shares unclassified and classified information with foreign governments as part of its authorized law enforcement, national security, and intelligence missions. Sharing with foreign partners, including the exchange of biographic and biometric information regarding known or suspected terrorists, requires both flexibility and adequate security precautions. As always, the FBI adheres to strict handling restrictions and ensures the protection of US Persons data.

The foundation of the FBI’s international program is the Legal Attaché (Legat) Program, which is administered by the FBI’s International Operations Division (IOD). IOD’s role is to support the FBI’s mission to defeat national security and criminal threats by building a global network of trusted partners and strengthening international capabilities. The FBI has Legat offices and sub offices in over 70 key cities around the world, providing coverage for more than 200 countries, territories, and islands. Due to their relationships with law enforcement and intelligence services abroad, Legats are familiar with investigative rules, protocols, and practices that differ from country to country. They are thus well-positioned to analyze and disseminate the intelligence that directly impacts the US national interests both domestically and abroad.

During 2011 the FBI revised its Foreign Dissemination Policy Implementation Guide (FDPG) to reflect several policy updates. The new version will include provisions for the dissemination of unclassified information (i.e. Controlled Unclassified Information (CUI), Law Enforcement Sensitive (LES), and For Official Use Only (FOUO) information). The FDPG will be posted on the FBINet Foreign Dissemination SharePoint site. The site provides a single reference point for the latest FBI and ODNI policy on foreign dissemination, and helps those who directly disseminate information to foreign governments by providing an extensive policies and procedures guide. The site also includes resources for FBI Designated Intelligence Disclosure Official (DIDOs) including current DNI foreign dissemination policies, FBI internal foreign dissemination policies, and many pertinent materials regarding foreign dissemination for those individuals authorized to share classified and unclassified information with foreign governments.

## **IV. MAXIMIZING AND INTEGRATING INFORMATION SHARING CAPABILITIES**

The FBI has highly-developed processes for collecting, analyzing, and sharing information through discovery, access, and collaboration capabilities. Intelligence and law enforcement provide the information; technology enables the FBI and its partners to find patterns and connections in that information. Through sophisticated, searchable databases and techniques, the FBI is surveilling and apprehending known and suspected terrorists and other criminals using biographical information, biometrics, travel histories, criminal histories, and financial records. That information is then shared with those who need it, when they need it.

### **Discover, Access, and Exploit Information Based on Mission Need**

**Law Enforcement Online.** The FBI's Law Enforcement On-Line (LEO) system provides secure, web-based communications accessible via the Internet and available to international, federal, state, local, and tribal law enforcement agencies. LEO enables the expedient sharing of sensitive information via professional special interest groups or topically focused dialogue, and provides access to an extensive array of FBI and other law enforcement agency databases and services. LEO gives law enforcement officers around the country access to unclassified information, intelligence reports, and alerts. It is interactive and provides state-of-the-art functions such as real-time chat capability, news groups, distance learning, and articles on law enforcement issues. LEO also offers a real time electronic command center known as the Virtual Command Center (VCC) for information sharing and crisis/incident management accessible at local and remote sites.

LEO offers a variety of services to the criminal justice community that create collaboration and cooperation among local, state, tribal and federal law enforcement personnel. Several accomplishments in 2011 enhanced the users' experience.

- LEO completed a search connection that gives users access to an Intelink search portal hosted by the Department of Justice.
- CJIS single sign-on capabilities became operational in 2011. Shared user and service directories with the Homeland Security Information Network (HSIN), Regional Information Sharing System (RISSNET), and Intelink provided a foundation for an integrated, cross-network set of directories to help users more easily locate experts in other agencies.
- Enhancements implemented to the VCC capability, such as displaying incidents by specific dates or times and improving refresh rates on the screens, improved critical real-time monitoring of operations from the local agency functions to national security needs. VCC provides an "Events Board" feature which allows information to be posted as the event occurs and allows users to post photographs, scanned documents, and any information deemed pertinent to the crisis. Whatever agency is hosting the VCC can allow access to individual persons or entire agencies if needed. Critical Incident Managers, such as emergency planners, now can have remote access to a crisis without

having to be on-scene. LEO members created 304 new VCCs in FY2011 and opened over 700 VCC event boards to collect, record, and disseminate information during an event.

- Enablement of Special Interest Group (SIG) and VCC restricted access capabilities allowed LEO to limit user access to certain areas on LEO, including email capability. This facilitates use of LEO by international law enforcement agencies.
- LEO members shared over 50,600 unclassified criminal activity and intelligence documents in FY2011.

With more than 55,100 active members, LEO continues to succeed because it evolves as law enforcement's needs evolve – from offering training support to expanding and improving the individual sites that make up the system. The LEO system is in the process of a technical refresh. Planned improvements include upgraded email, search, and chat capabilities, and language translation abilities. Future plans include integration into an enterprise portal environment.

**Law Enforcement National Data Exchange.** The FBI CJIS Division is the focal point for some of the most important and relevant criminal history databases used by law enforcement. One such database, the CJIS-developed National Data Exchange System (N-DEx) is a criminal justice information sharing system providing nationwide connectivity to disparate local, state, tribal, and federal systems. It is the first nationally-scaled criminal justice information-sharing platform. N-DEx provides a secure, online national information sharing system to the criminal justice community for their data, including incident, arrest, booking, incarceration, probation, and parole reports.

The N-DEx resulted from collaboration among local, county, state, tribal, and federal criminal justice communities. The application of N-DEx capabilities provides the missing links and creates partnerships that lead to more effective investigations that will help disrupt and apprehend individuals and organizations responsible for criminal activities and national security threats.

The N-DEx Program's goal is to provide the right information (incident and case reports, arrest, incarceration and booking data, probation and parole data), to the right users (approved criminal justice agencies), right now (near real time). The Program realized many of these goals when N-DEx reached full operational capability in March 2011 with CJIS delivery of the final increment of the system. N-DEx will continue to augment its capabilities to keep pace with the needs of the criminal justice community. Its third and final increment offers more advanced tools, numerous enhancements, a better user experience, and added additional data sets from the criminal justice community.

The N-DEx Program continued to receive recognition in 2011 for its ground-breaking information sharing efforts. The N-DEx Law Enforcement Information Exchange (LInX) Northwest Team was awarded the FBI Science and Technology Branch Innovation Award, established to recognize contributions within the Branch that were novel, practicable, and had measurable impact. This team made significant contributions to integrating the LInX initiative into N-DEx, fostering sustained participation, mutual understanding and cooperation.

N-DEx was further honored by the Association for Enterprise Information, which presented the N-DEx Program Office with its “Excellence in Enterprise Integration Award” for outstanding achievement in the application of enterprise integration resulting in innovation, greater customer value, visionary strategy, and cultural change. This is the first time that a non- DOD agency has received this award. The AFEI President said N-DEx’s endorsement by the International Association of Chiefs of Police and the National Sheriffs' Association demonstrated its real-world ability to connect the dots. The award recognized N-DEx’s status as a powerful and relevant tool to solve crime in ways not previously available.

In addition, the N-DEx Program Office was recognized by the Armed Forces Communications and Electronics Association Bethesda Chapter with a Government-wide Initiatives Excellence Award for Outstanding Achievement for Law Enforcement.

Each year, the Integrated Justice Information Systems (IJIS) Institute recognizes technical innovation that has contributed significantly to the advancement of information integration and interoperability in a public safety, justice, and homeland security project or program. A central element to this award, which is sponsored by Emergency Management Magazine, is that nominated projects must be justice and public safety efforts that have contributed significantly to the advancement of integration and interoperability by offering a solution that can serve as a model to other justice and public safety public sector agencies.

The N-DEx Program received the 3<sup>rd</sup> Annual IJIS Institute Innovation award at the National Forum on Criminal Justice and Public Safety, which is a conference jointly managed by the National Criminal Justice Association, the IJIS Institute, and the Bureau of Justice Assistance. This was the first time a federal agency has received this award.

Internal to FBI, the Chief Information Sharing Officer was instrumental in redefining corporate policies regarding the utilization of N-DEx to create coordinated, comprehensive, transparent, and consistent policy and governance for the information sharing activities of the FBI with its external partners. The policy changes should have the effect of making FBI information sharing more robust, institutionalizing the utilization of N-DEx within the FBI, while providing tools to executive managers to better measures of sharing activities.

At the end of November 2011, the N-DEx system had over 124 million searchable records with more than 780 million entities (persons, places, things, and events), more than 24,000 total users, and receiving data from 36 data sources representing over 4,100 submitting agencies.

N-DEx reports monthly the percent of population served by N-DEx via state and local law enforcement participation as a metric on the Enterprise Strategy Management System scorecard for the Director of the FBI. It is projected that 50% of the United States population will be served by N-DEx via state and local law enforcement participation as of the end of fiscal year 2012.

Also in November 2011, FBI Director Robert S. Mueller, III, approved the CJIS Advisory Policy Board (APB) recommendation to expand the accepted system access and acceptable use policy of N-DEx beyond law enforcement to include criminal justice agencies. This further enhances

the ability for N-DEx to support the criminal justice community by broadening the user base to include agencies supporting probation, parole, corrections, courts, prosecutors, and dispatchers. Access to N-DEx had been limited to law enforcement agencies during piloting and prototyping. To support record-owning agencies' need to responsibly share their information, the N-DEx Program developed a sophisticated set of tools allowing criminal justice agencies a great deal of flexibility to share their information with whom they need in a way consistent with their mission, legal, and policy requirements.

In addition, DHS is poised to share information from their Law Enforcement Information Sharing (LEIS) system with the criminal justice community via N-DEx. Making DHS information available via N-DEx is another significant milestone N-DEx in efforts to support the national sharing of unclassified criminal justice information.

As a consequence of these activities and approval of the APB recommendation, the N-DEx Program Office is requesting to change its name from Law Enforcement National Data Exchange to Criminal Justice National Data Exchange.

In an era where information sharing is a critical mandate across the criminal justice community, the N-DEx system is well positioned and ready to efficiently and effectively serve criminal justice agencies for decades to come as its only nationally-scaled information sharing system.

**Data Integration and Visualization System (DIVS).** A major enhancement to FBI analytic capabilities, and an enhancement to facilitate the efficient sharing of FBI information with other authorized parties, the Data Integration and Visualization System (DIVS) provides a single interface through which agents and analysts can search multiple FBI data repositories, filter results, and quickly locate information most pertinent to their work. DIVS was created to make more efficient the access and use of all this data, to prioritize and more effectively integrate over 200 datasets across the Bureau. One of the Director's top initiatives, DIVS was deployed to the FBI in late 2010 and enhanced in 2011 to include greater access to databases, improved search capabilities, and better connectivity to analytic tools.

The DIVS program provides single sign-on, role-based access controls to analyze and link all FBI data that the individual user is lawfully allowed to access. In the future, this system will also provide the means to efficiently feed data from the FBI Secret network to the FBI Top Secret system. For the first time in FBI history, agents and analysts will have the ability to effectively search and study foreign intelligence data, Human Intelligence source information, law enforcement data, and investigative reports in a single sign-on environment. This capability enables more effective discovery within the 1.73 billion indexed records and 11.1 terabytes of searchable data housed in FBI and other government agency data sources at FBI. As a result, using DIVS saves time and facilitates more efficient sharing of relevant FBI information with other intelligence and law enforcement partners. It will also ultimately help reduce or eliminate redundant data systems. DIVS, currently available only to FBI personnel, will enhance the capability of the FBI to more effectively analyze and share its information.

**Next Generation Identification System.** In 2011 the CJIS Division started using new technology to enhance the FBI's ability to more quickly and efficiently identify criminals and

terrorists. The Next Generation Identification (NGI) system is incrementally replacing the Integrated Automated Fingerprint Identification System (IAFIS), which provides automated fingerprint and latent search capabilities to more than 18,000 law enforcement and criminal justice partners, 24 hours a day, 365 days a year. Incorporation of the NGI Program's Advanced Fingerprint Identification technology into the 10-year-old IAFIS system allowed faster processing of fingerprint transactions and increased the accuracy of fingerprint searches from 92.0 to 99.6 percent.

### **Enhance Capabilities for Collaboration and Information Sharing**

**The Biometric Center of Excellence.** The FBI-led Biometric Center of Excellence (BCOE) is tasked with technical and programmatic leadership in the field of Biometrics. This is accomplished through technical stewardship of software and hardware prototypes; information and knowledge exchanges through conferences, meetings, and training; direct interaction with federal, state, and local law enforcement; management of technology projects with academia and the private sector; and a highly visible presence in biometric community events. The BCOE shares technology, selected data, and biometric-centric domain knowledge in a bi-directional way with its stakeholders and trusted partners through technical exchanges, specialized working relationships, and through active point-of-contact interaction.

In 2011, the BCOE sponsored 24 applied biometric research projects concerning fingerprints, deoxyribonucleic acid (DNA), face, voice, and multimodal recognition. Fourteen of these projects were co-sponsored with federal agencies, such as the National Institute of Standards and Technology, the Department of Defense, and the Department of Homeland Security; ten were cosponsored with academia.

- One project, the Automated Face Detection and Recognition (AFDAR) prototype, improves the ability of investigative agencies to analyze large collections of lawfully-collected images and videos for potential evidence.
- In another project, recent technological advances, sponsored by the BCOE, are being employed in development of portable Rapid DNA machines that enable identification of individuals by their DNA in the field.
- The BCOE also initiated the TattooID Pilot, which will enable users to initiate searches using a test image to find similar images; results of the pilot program will be evaluated and incorporated into technology enhancements. The algorithms used in this prototype were shared with the White House Innovation and Infrastructure Initiative to facilitate development of an interoperable wireless network for law enforcement that enables use of mobile devices to access resources like the TattooID tool.

Furthermore, the BCOE transitioned the facial searching concept to an operational service. This service allows images to be submitted to a facial examiner who processes and compares the images with numerous facial recognition systems and databases. Results are then provided as investigative lead information.

The BCOE sponsored 20 collaborative events with US government agencies, industries, state and local agencies, and international law enforcement. In addition, they developed and shared

training courses, including introduction to Biometrics Computer-Based Training; Facial Comparison and Identification Training; and Quick Capture Platform Just-in-Time Training.

The BCOE combines knowledge and experience of staff from the FBI's Laboratory Division, the Operational Technology Division, and the CJIS Division. Representatives from these three FBI Divisions continue to develop collaborative partnerships with law enforcement, academia, and private industry worldwide. Finally, the new BCOE *Biometric Quarterly* provided FBI agents with news and updates about biometric technologies, prototypes, and services.

**The eGuardian System and Suspicious Activity Reporting.** The FBI Counterterrorism Division's (CTD) Guardian Management Unit continues to support the unclassified version of its Guardian program. This information sharing platform, called eGuardian, was developed to help meet the challenges of collecting and sharing information on terrorism-related activities with law enforcement agencies across various jurisdictions. Accessible via LEO, the system facilitates situational awareness of potential terrorist threats and suspicious activity with potential nexus to terrorism by allowing law enforcement agencies to combine new Suspicious Activity Reporting (SAR) along with existing (legacy and NSI) SAR reporting systems to form a single information repository accessible to thousands of law enforcement personnel.

The eGuardian system is a valuable information sharing tool, assisting in law enforcement collaboration and threat mitigation. The information captured in eGuardian is also migrated to the FBI's internal Guardian system, where it is assigned to the appropriate Joint Terrorism Task Force (JTTF) for any further investigative action. Of the roughly 14,000 incidents entered into eGuardian, 417 incidents have been converted to either Preliminary or Full Investigations.

The system was modified and improved in 2011 based on feedback and suggestions from users. Modifications were also made to facilitate better system and information incorporation into the Nationwide SAR Initiative (NSI). The FBI modified its internal business processes and began pushing unclassified Guardian incidents to eGuardian in 2010/early 2011, ensuring full FBI participation in the eGuardian system and the information sharing process; over 5,000 unclassified incidents have been pushed from Guardian to eGuardian and the NSI Shared Space.

The number of eGuardian agencies and users continued to grow in 2011, and so did training requirements. FBI continued actively training mission partners in appropriate use of the eGuardian system. In 2011, vetted personnel in numerous agencies received training from FBI personnel as follows:

DOD	701
FBI	164
DHS	104
DOJ	28
DOS	10
Other Federal	43
<u>Other Non-Federal</u>	<u>956</u>
TOTAL	1,305

As of November 2011, there were over 1200 member agencies with a total of approximately 4000 users in the system. These member agencies are local police and sheriff departments, state-level agencies and fusion centers, tribal law enforcement, campus law enforcement, and federal agencies, including law enforcement components within the DOD.

**Terrorist Screening Center (TSC).** Hosted and managed by the FBI, the TSC continued work on a number of initiatives in 2011 to streamline information sharing processes among the major counterterrorism centers providing comprehensive watchlist support to the US Government while safeguarding the privacy, civil rights and civil liberties of Americans.

The Editable Terrorist Screening Database (TSDB) provides a capability that supports record-by-record reviews of Known or Suspected Terrorist (KST) records. An initiative that improved the process for correcting data errors found in KST nominations was implemented in 2010. This initiative was accomplished as a project that involved coordination of internal TSC units and with our external NCTC partners. As data are validated, the system updates the record date and sends updates to downstream customers as appropriate. Both the TSC and NCTC believe that data quality has improved and there is closer coordination between the two organizations on a daily basis. Downstream customers are receiving edited data faster than they were previously.

In 2011, the TSC incorporated additional biometric identifiers into the TSDB application that allows TSC to import, hold, and export biometric data. Enhancements were achieved as several incremental steps:

- Capability to hold biometrics data from TIDE Interim Biometrics Repository (TIBR). A full set of biometrics modalities can be received from TIBR that may include facial images, iris scans, and fingerprints. These data are also cross-checked against NCTC TIDE biographic data. All biometric and biographic data are associated together for KSTs. Over 36,000 TIBR files were imported to TSDB; data validation checks reported corrupted files and unassociated records to TIBR and NCTC.
- Capability to hold biometrics data for unknown persons. TSDB could hold facial photos from unknown persons; this capability was enhanced to hold latent fingerprints.
- Capability to assign a National Unified Identity Number (NUIN) was added to TSDB. The NUIN numbers are provided to NCTC to update TIDE records.
- Capability to export data to downstream screening agencies. TSDB provides KST facial photos to Department of State for its Facial Recognition System, to the NCIC, and DHS Watch List System (WLS). TSDB has built in the ability to extend WLS data to include iris scans and fingerprints; the capability can be turned on as soon as a downstream customer is identified. TSC reviewed the enhancement of WLS biometrics data with DHS, Customs and Border Patrol (CBP), and US Visit. The TSC also developed a revised interface control document to provide the enhanced biometrics data.

Remote Access is a capability for providing KST watchlist data to screening agencies. The NCTC was provided access to this on-line query tool to support their daily work. NCTC analysts require updated information on watchlist assignments; previously this data was requested by faxed requests to the TSC Call Center. Remote Access allows NCTC analysts to

look up the data that they require and to carry out quality assurance checks. The response by NCTC has been very positive; over 75 persons use Remote Access.

Encounter data are being provided to NCTC. The positive encounters are provided to NCTC and are loaded directly into the NCTC TIDE queue. These data are processed daily and made available to the Intelligence Community through TIDE OnLine. DHS components receive encounter data using voice, email, and special purpose reports. TSC and DHS have long-term plans for two-way electronic exchange of encounter data with DHS components through the DHS WLS. This initiative will be pursued by DHS after it has fully implemented the sharing of watch list data with DHS components.

This data is also provided to several FBI divisions, including the FBI Foreign Terrorist Tracking Task Force (FTTTF) and Special Technologies and Applications Office (STAO).

Staff from FBI developed a Terrorist Screening System (TSS) CONOPS for TSC information technology (IT) systems. This provides program objectives that provide greater specificity to the design of TSS capabilities. The CONOPS review provided internal units the opportunity to comment and influence IT capabilities. This document provides a foundation for the prioritization of specific IT development tasks across the TSC.

The TSC worked with DHS and CBP to design and implement the Watch List System (WLS). This system provides significant enhancements to the KST watch list data that are utilized by DHS components. The new capabilities include the following: greatly expanded set of watch list data for screening agencies; real-time delivery of watch list data as soon as the nominations processing is completed; and a two-stage data reconciliation capability that provides a daily validation that the TSDB and WLS data are accurate and complete. TSC provided extensive testing support to DHS to ensure that this project was completely successful. The WLS was put into production on 7/7/2010 and currently provides immediate feeds to CBP TECS and the Advance Passenger Information System (APIS) for port of entry and airline screening. The data are moved from TSDB to WLS to CBP TECS and APIS, and are validated within two minutes. Future efforts will extend the data delivery to Transportation Security Agency (TSA) components, DHS Intelligence and Analysis, ICE, and US Visit. This is a major capability enhancement for KST watchlisting.

Enhancements were incorporated into the Encounter Management Application (EMA) that increased the data fields collected and improved the data quality. A data review function was added that supports data quality reviews.

TSC previously implemented a TSA Secure Flight data export. Since that implementation, TSC has provided operational support to TSA to resolve data questions and data refresh support. TSA requested a new watch list code, and Expanded Selectee (ESEL) as follow-on to the new Watchlist Guidance policy. TSC is actively working on a modification to the current Secure Flight export to include ESEL records. A draft Intelligence Community Directive was also provided to TSA for review.

**FY2011 Accomplishments:**

TIDE2 Interface Control Document	NCTC is implementing a revised TIDE application that sends nominations to TSC. TSCU drafted the ICD and sample messages for NCTC and TSC development efforts. Interagency development efforts continued through deployment in 12/2010.
DHS Watch List System Export	TSC implemented a transactional interface with DHS WLS that currently feeds two DHS agency systems and will replace five other data feeds to other systems. Data are being screened in downstream systems within two minutes of release by TSC operations.
Encounter Exports to NCTC and FTTTF	TSC implemented the first exports for positive terrorist encounters to the National Counterterrorism Center and the FBI Foreign Terrorist Tracking Task Force. Daily updates are accessible by the Intelligence Community via NCTC's TIDE OnLine system.
TSA Secure Flight Export Enhancement	TSA requested an expansion to its export data based on new White House Watchlisting Guidance. A draft ICD was prepared by TSC and reviewed with TSA at a meeting on 08/24/2010.
Release Terrorist Screening Database 2.8 – DOS and Biometrics	TSDB 2.8 provides DOS with enhanced data using a transactional interface (similar as DHS WLS). The version also delivers enhanced biometrics to DOS, NCIC, and DHS.

**V. MAXIMIZING AND INTEGRATING CAPABILITIES TO SECURE INFORMATION**

In 2011 the Federal Government identified several measures considered critical to protecting the nation's network of information systems: interoperable identity management; user authorization and access; and auditing and monitoring to safeguard information, improve oversight, and protect information networks from external and insider threats. Initiatives already funded and underway at the FBI for implementation on internal networks address some of these measures. Work began in other areas to address the unmet requirements.

**Identity Management**

The FBI has vigorous identity management programs across its internal networks. Staff worked closely with Federal partners throughout 2011 to advance development and implementation of Identity, Credential, and Access Management (ICAM) capabilities across the Federal unclassified networks, enable interoperability with FBI networks, and to promote information sharing, and efficiencies of scale across all agencies within the Federal Government. The updated FBI CJIS Trusted Broker in 2011 became a source of single sign-on capability for numerous Information Sharing Environment partners, allowing LEO users to access the Director of National Intelligence's Intelink-U, RISSNET, and other systems. Further, the CJIS Trusted Broker allows RISSNET users to access the Joint Automated Booking System (JABS) and Intelink-U without requiring separate accounts. The SBU partnership plans to further enhance interoperability among the partner systems, including the fourth SBU partner, Homeland

Security Information Network (HSIN). The partnership will build on the identity management schema to enable cross-partner federated search, discovery and retrieval. In addition, work continues to standardize system security practices including user account vetting and account de-provisioning. System certification and accreditation reciprocity is another area of technical as well as policy collaboration.

The Sentinel program also relies heavily upon identity management using role-based access controls to ensure agents, analysts, and supervisors have appropriate access, retrieval, and information management permissions.

Several high-visibility events in 2010 and 2011 caused shift in focus to enhance traditional information security controls with advanced capabilities on classified networks to achieve a common level of assurance in information handling and sharing. In response to these and other drivers, the Federal CIO Council / ICAM Sub-Committee (ICAMSC), the National Security Staff / ISA IPC's Assured Secret Network Interoperability (ASNI) Working Group, and CNSS's Identity and Access Management (IdAM) Working Group collaborated to evaluate the applicability of ICAM capabilities on US Secret networks. This analysis was prepared for the ISA IPC review with strong FBI cross-directorate participation. The analysis will be used to inform new standards for Secret networks.

### **User Authorization and Access**

User authorization and access to FBI automated information systems has been enhanced by the implementation of all IT System Access Requests into the Enterprise Process Automation System (EPAS). EPAS, a commercial off-the-shelf-based software tool suite, serves not only IT system access but also agent hiring, awards, and clearance processes. The tool suite provides the FBI with the capability to model current paper-based processes and then automate them into more efficient electronic workflows. Resultant workflows can then be modeled and tested to create more effectively managed, monitored and improved processes as organizational changes occur.

Based on specific role based access to the System Access Requests component of EPAS, users and administrators now follow standardized processes across the enterprise to facilitate access to specific IT resources. Tracking and management of approved system access authorizations, as well as the revocation of system access, is highly documented, controlled and reportable through the EPAS reporting features.

The IT Branch had previously implemented the use of a common access card (CAC) to improve the authorization and access checks on FBINet. Work continued to ensure that the FBI program was commensurate with standards being adopted across the DOD. Implementation helps FBI ensure appropriate authorization and access control, and meets structural reforms called for under Executive Order 13587.

Key to FBI plans is establishment of an overarching policy governing data access and access rules management. An Information Sharing Team under the direction of the ISPB invested tremendous effort in developing a comprehensive Enterprise Data Access Policy and rules

registry plan. This policy, when approved by the ISPB, will govern procedures and policy for access to all FBI systems.

### **Audit and Monitoring**

The FBI has been a leader across the federal government in audit and monitoring. Several of its practices are considered the “gold standard” in the federal system. All FBI IT systems must now participate in enterprise level integrated system security monitoring. Specific audit and monitoring requirements are determined based on published standards related to the IT system’s criticality to the FBI mission prior to being authorized on the FBI’s computer networks. Work continues to enhance FBI ability to monitor all systems in the field as well as share audit information appropriately with external partners.

Throughout 2011, a cross-directorate team reviewed internal policies and procedures to enhance accountability and decrease risk to information in FBI’s classified networks as part of a long-term comprehensive, enterprise Data Protection Program. Security Division and IT Branch initiated a pilot program testing procedures to decrease data transfer, minimize the use of removable electronic storage devices, and encourage use of enterprise cross-domain solutions. This program supports audit and monitoring as well as the FBI’s “insider threat” detection and monitoring program.

## **VI. STRENGTHENING THE GOVERNANCE FRAMEWORK**

The FBI is committed to sharing timely, relevant, and actionable intelligence with its mission partners as part of its national security and law enforcement missions. These relationships are governed through both internal and external boards and committees, which collaborate to strengthen the framework to optimize responsible information sharing while protecting civil liberties and privacy.

Activities in 2011 reinforced the concept that policy and governance are critical to information safeguarding and secure sharing. The National Security Staff sponsored anew efforts among the Executive Departments to enhance information sharing. The FBI participated in several Interagency Policy Committees (IPCs) that affect the manner in which the federal government shares information. The Program Manager for the Information Sharing Environment is co-chair of one of those IPCs and ensures that state, local, territorial, tribal, and private sSector equities are included in policy decisions associated with counterterrorism, weapons of mass destruction, and homeland security. The Office of the Director of National Intelligence (ODNI) sets ground rules for the sharing of sensitive intelligence among the members of the Intelligence Community, including the FBI. The Department of Justice assumed new roles, and continues to sponsor other initiatives that enhance FBI information sharing. Within the FBI, the Information Sharing Policy Board provides senior-level policy coordination while the CISO provides full-time oversight and coordination of information sharing issues.

## **FBI Governance of Information Sharing**

A number of entities have been established within the organization to further this commitment. They work to codify information sharing principles, to engender an information sharing culture, and to enable information sharing practices and operations.

**Information Sharing Policy Board.** The ISPB, chaired by the Executive Assistant Director of the National Security Branch (NSB), is the executive-level forum for policy review and approval. It is the FBI's primary authority for information and intelligence sharing policy. Membership includes executive management from all operational and support staff across the Bureau, including the Office of the General Counsel and the Corporate Policy Office. The ISPB meets quarterly. The CISO serves as Executive Secretary of the ISPB and acts as principal advisor on information sharing activities.

Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," heavily influenced ISPB activities in 2011. Review of agency implementation criteria showed that FBI is meeting all minimum compliance standards, and is considered a model for other agencies to emulate regarding "insider threat protection," and the overall implementation to "safeguard without preventing information flow." The Director's Office named the CISO as the FBI Senior Official charged with overseeing classified information sharing and safeguarding efforts for the agency. The Board agreed that "minimum compliance" is not sufficient, and the FBI needs to continue progress. Finance Division, Information Technology Branch, Security Division, and Counterintelligence Division collaborated to identify and redress the unfunded requirements to meet structural reforms called for in Executive Order 13587 implementation guidance.

Publication of implementation guidance related to EO 13556 regarding Controlled Unclassified Information, and Intelligence Community Standard 501-27 (Collection and Sharing of Audit Data) also influenced review of FBI policy. The ISPB directed communications to Field Offices to ensure general awareness of new executive orders, implementation guidance, and IC policies, as well as implications for FBI reporting and information dissemination.

The ISPB directed and approved several policies in 2011 that impact information sharing: corporate policy regarding FBI staff participation in collaborative environments; policies updating and explaining access to FBI information systems in other government agencies as well as state and local fusion centers; policy regarding access attribute designation for FBI personnel who access IC systems and information; policy on appropriate dissemination of raw and finished intelligence; and memoranda of understanding with other government agencies related to sharing information contained within FBI databases. The Security Division established a new comprehensive security framework and implementation guidance, encompassing information and system security, to enable secure sharing. In addition, the Board addressed issues related to insider threat, development of a data protection program, and enterprise information access by both internal and external trusted staff.

**Access Policy Group.** The Access Policy Group (APG), chartered by the ISPB, is a standing group that supports, carries out directions from, and makes recommendations to the ISPB. Representatives of all FBI Divisions coordinate issues and vet policy for executive review and approval. Chaired by the CISO, the APG performs assessments for and makes policy recommendations to the ISPB on using various aspects of internal and interagency information sharing issues. These include such matters as IT and non-IT aspects of user access policies and data source approvals for FBI analytic, intelligence; and investigative systems and tools. It serves as the primary point of coordination for FBI IT and operational components working on different facets of internal and interagency information sharing. Under the APG, the FBI uses multiple Information Sharing Teams (ISTs) to work specific issues.

In 2011, the APG focused on data access and protection. Specifically, efforts centered on developing an enterprise data access policy and ensuring that information and accesses are properly secured. Policies regarding enterprise data access (based on user role attributes), removable electronic storage media, cross domain data transfer, and information system security framework were written and in final approval review by the end of the year. Coordination continued on improving policy and technical mechanisms for loading documents to the Library of National Intelligence, on protocols for developing access controls for newly-issued case classifications, guidance on proper use of information markings (classified and unclassified), and revision of information sharing/system connectivity with other government agencies. All of these reviews were considered for impact on mission, technology, security, and legal constraints.

**Information Sharing Teams.** ISTs are ad hoc working groups formed to conduct specific or targeted assessments in response to ISPB/APG requirements relating to FBI analytic, intelligence, and investigative systems, data and tools. They also work in conjunction with the FBI Office of Congressional Affairs to formulate responses to Congressional requests. Work in 2011 continued on the following:

- Enterprise Data Access Policy and Rules Repository.
- Controlled Access and Information Sharing on FBI Intranet Websites.
- Review of Intelligence Community Standards related to information access and sharing, including collection and sharing of audit data, requirements for digital identity.
- Automated Case Support (ACS) System and Sentinel Data Restriction Policy, and
- National Counterterrorism Center Information Sharing Initiative.

**Chief Information Sharing Officer.** The FBI CISO position was created to build a unified and effective information sharing environment within the FBI. As the principal advisor to FBI executives on information-sharing issues, the CISO provides policy direction on information sharing to FBI Divisions and leads coordination of FBI information sharing activities. Within the FBI, the CISO chairs FBI forums and groups to advocate for appropriate information sharing and to identify emerging issues or gaps in communication. The CISO serves as Executive Secretary of the ISPB and Chair of the APG.

In 2011, the CISO provided FBI representation to numerous interagency policy and information-sharing organizations, including several White House National Security Staff Interagency Policy Committees (IPCs) related to information sharing and security; the Intelligence Community

Information Sharing Steering Committee (IC ISSC); Department of Justice meetings related to the Law Enforcement Information Sharing Program (LEISP) and the Global Justice Criminal Intelligence Coordinating Council (CICC); and other senior groups. The CISO spoke frequently at conferences and public discussions on information sharing topics. The CISO facilitated, monitored, and reported on interagency information-sharing initiatives between the FBI and other organizations (which comprise federal, state, local, tribal, foreign, and private partners), identifying issues and inconsistent policies, making recommendations, and informing policy creation/revision. The CISO also contributed to the preparation of Congressional testimony and other public statements by FBI senior leadership on information sharing topics.

**CJIS Advisory Policy Board.** The FBI established the CJIS Division to serve as the focal point and central repository for criminal justice information services within the FBI. Most of these are information sharing systems, managed for the benefit of local, state, tribal, federal, and foreign criminal justice agencies. They include the Next Generation Identification (NGI); Integrated Automated Fingerprint Identification System (IAFIS); N-DEx; LEO; NCIC; National Instant Criminal Background Check System (NICS); and the Uniform Crime Reporting (UCR) Program.

The CJIS Division's management responsibilities include the operation of existing systems and the development of new technologies. The FBI established the CJIS Advisory Policy Board (APB) to obtain the user community's advice and guidance on the development and operation of all of these programs. The philosophy underlying the advisory process is one of shared management; that is, the FBI along with local, state, tribal and federal data providers and system users share responsibility for the operation and management of all systems administered by the FBI for the benefit of the criminal justice community. The APB is composed of thirty-four representatives from criminal justice and national security agencies and organizations throughout the United States; created to serve as the responsible entity for reviewing appropriate policy, technical, and operational issues related to CJIS Division programs. Subsequent to their review, the Board makes recommendations to the FBI Director. Many of these recommendations impact information sharing. The CISO and CJIS work very closely together to ensure awareness and consistency of APB and ISPB policies.

### **Interagency Governance**

The FBI participates in many external organizations, programs, and initiatives to facilitate information sharing and the fusion of information into actionable intelligence. Information sharing relationships exist at all levels between and among federal agencies and the IC; state, local, and tribal agencies; private sector businesses, academic institutions, and associations; and international partners. These organizations work within their communities to enhance communications, coordination, and cooperation on terrorism and threat matters in support of the shared missions of public safety and the national security of the United States.

### **Senior Information Sharing and Safeguarding Steering Committee.**

A critical component of sharing governance in 2011 is the Steering Committee created by EO 13587 to address sharing and security concerns in the aftermath of the WikiLeaks events. This committee, co-chaired by NSS Deputy Homeland Security Advisor and the OMB Federal CIO, is responsible for guidance and oversight of federal efforts to improve responsible sharing and safeguarding of classified information. The FBI is regularly represented in this committee by

both the Associate Executive Assistant Director of Information Technology Branch and the FBI CISO. In addition, the FBI has assigned personnel to each of the Committee's elements established to carry out the policy and guidance of the Steering Committee: the Executive Agent for Safeguarding; the Insider Threat Task Force; and the Classified Information Sharing and Safeguarding Office.

**Information Sharing and Access Interagency Policy Committee.** The Information Sharing and Access Interagency Policy Committee (ISA IPC) serves as the National Security Staff focal point for issues related to information sharing. Its focus extends beyond terrorism-related issues to a broad range of information sharing issues which impact national security. The ISA IPC is charged with leading an interagency policy process to identify information sharing and access priorities to more fully address the needs of federal, state, local, tribal, and private sector stakeholders while protecting privacy and civil liberties.

The IPC has five sub-committees: Watchlisting and Screening; Fusion Centers; Suspicious Activity Reporting; Privacy, Civil Rights and Civil Liberties; and Information Integration. The FBI actively participated in the ISA IPC itself, in the sub-committees, and in focused working groups in 2011. The FBI CISO regularly represented the FBI and its equities at the general ISA IPC meetings. Much of the work occurred at the sub-committee and working group levels.

The Fusion Center sub-committee was co-chaired by an FBI Deputy Assistant Director (DAD). In 2011 this sub-committee continued to provide executive oversight for the National Fusion Center Program Management Office and issues related to Fusion Center Baseline Capabilities.

The Suspicious Activity Reporting sub-committee was also co-chaired by an FBI DAD. This group provided executive oversight for the Nationwide SAR Initiative (NSI) Program Management Office and collaborated on policy with the other sub-committees.

The Watchlisting Sub-Committee reviewed watchlisting business processes to ensure continued improvement in information sharing among the major counterterrorism centers while safeguarding the privacy, civil rights and civil liberties of Americans. The Counterterrorism Division provided subject matter experts as well as operational expertise for this group.

The CISO, with concurrence and support of the Information Technology Branch (ITB) and the Directorate of Intelligence, represented FBI at the Information Integration sub-committee. This group had two very active working groups. Representatives from ITB and the CJIS Division participated in the aggressive schedule set by the Assured Sensitive But Unclassified (SBU) Interoperability Working Group to link four SBU networks, ensure email and services could be exchanged across them, documented Segment Architecture Guidance, and facilitated single sign-on capability for trusted users. The CISO collaborated with DOJ in the second working group, Assured Secret Network Interoperability, which studied requirements for system interoperability (including state and local fusion center information needs), and worked closely with other federal partners in studying potential adoption of Federal Identity Credential and Access Management standards on the classified networks.

**Office of the Program Manager for the Information Sharing Environment.** The FBI works closely with the Program Manager for the Information Sharing Environment (PM-ISE) throughout the year on issues related to the ISA IPC, drafting EO 13587, and establishing new activities related to that order. The PM-ISE worked with FBI, the Department of Homeland Security (Intelligence and Analysis), and other partners to ensure fusion centers continue to grow in capabilities and capacity. The PM also worked with FBI and the Nationwide Suspicious Activity Reporting Initiative (NSI) Program Management Office to ensure fusion centers have necessary capabilities to receive, fuse, report, and share information appropriately with Joint Terrorism Task Forces and other NSI partners.

Different FBI offices participated in the interactions with PM-ISE depending upon the issue being addressed. The CISO coordinated many of these interactions and maintained familiarity with the rest to ensure coordination of FBI internal and external activities.

**Intelligence Community Information Sharing Steering Committee.** The CISO represented FBI at the Intelligence Community Information Sharing Steering Committee (IC ISSC), which collaborated on information sharing issues including policy, budgetary, process, and technical aspects. The IC ISSC issued an Information Sharing framework containing specific goals and objectives designed to create unity of effort in information sharing spanning the five critical building blocks of governance, policy, technology, culture, and economics. The IC ISSC also worked closely with ISA IPC and DOD to align and improve information sharing across the Federal Government and with state, local and tribal entities. The Information Sharing Executives from each IC element served as representatives to the IC ISSC.

## **VII. PROMOTING A CULTURE OF RESPONSIBLE INFORMATION SHARING**

Information sharing activities at the FBI embody the commitment to operate at all times under the rule of law, respectful of privacy, civil liberties, and human rights, and in a manner that retains the trust of the American people. The FBI NISS addresses the cultural and technological changes required to move the FBI to a “sharing” culture. All elements of FBI’s law enforcement and national security components rely upon effective acquisition and sharing of information for successful execution of mission. This inherent dependence is expressed in a number of ways. The FBI continues its cultural transformation through recognition and adoption of best practices and evolving technology standards of both the intelligence and law enforcement communities.

### **Incorporating Information Sharing**

The FBI identified fundamental principles and enduring values essential for responsible sharing several years ago in its National Information Sharing Strategy. The strategy provides the foundation to shape and implement information sharing initiatives with the FBI’s many mission partners, including federal agencies, state, local, and tribal officials, foreign government counterparts, and private sector stakeholders. The NISS document is organized around three goals:

- Reinforce the emerging culture of information sharing by emphasizing the benefits of active information and knowledge exchange.
- Make information sharing easier through the focused use of information technology and policy.
- Make information sharing more effective.

The NISS is updated annually to ensure its relevance is understood in an ever-changing operational environment. The values expressed in the NISS, however, are constant and have become embedded in several foundational initiatives. This was evident in the manner in which FBI dealt with threat information in the past year specifically related to the tenth anniversary of 9/11. The FBI consciously prepared for the anniversary with several objectives in mind:

- Join forces from the very top to ensure there is clear understanding of roles and unity of purpose at all levels of law enforcement, intelligence, and public safety officers.
- Bring in state, local, tribal, and private sector (wherever possible) early for joint presentation of situational awareness briefs by seniors from responsible agencies.
- Ensure all aspects of law enforcement are used.
- Use technology smartly to improve efficiency and communication.
- Issue jointly-sealed information products, quickly and concurrently, that convey actionable information at classification levels that can be broadly shared.
- Ensure contact information is provided on each product, and solicit feedback.
- Provide follow-through or summary communications to wrap-up the event.

### **Ensuring Accountability**

The FBI's Senior Executives are rated on "Collaboration and Integration" as part of their performance evaluations, indicative of the Bureau's interest in rewarding information sharing efforts. In addition, each Special Agent and Intelligence Analyst has information sharing elements included in annual performance work plans.

### **Training and Awareness**

Numerous training courses required by the FBI for staff and contractor personnel address secure sharing of information. Annual Information Assurance, handling of US Persons data, handling of controlled or sensitive unclassified information, and Domestic Investigations and Operations Guide (DIOG) and other courses refresh permanent and contractor staff understanding of appropriate and secure sharing. Elements from these courses are included in training on use of various FBI information sharing systems such as LEO, N-DEx, eGuardian, and DIVS.

The Information Sharing Technology Speaker Series and Knowledge Week seminars on Intelligence Community Information Sharing reinforce this training with demonstrations of real-world application of the concepts.

For many years the FBI has participated in National Level Exercises (NLE), testing coordination and integration of various processes at the national level in response to a disaster or crisis. The

growing importance of information and intelligence analysis integration at FBI led to the creation of a new position in 2011, the NLE Coordinator, to ensure that the FBI's intelligence component is fully incorporated in process planning for real-world interagency contingency response.

## **Awards**

The FBI is one of three federal agencies that offer agency-specific incentives to encourage information sharing, according to the Program Manager for Information Sharing Environment 2011 Annual Report to The Congress. Four individuals from across the FBI received the Chief Information Sharing Officer Award in 2011. This award was created to enhance awareness of information sharing goals and the central role they play in the FBI's National Security, Intelligence, and Law Enforcement missions.

- In September 2011, based on a personal commendation from the Commander of the California State Terrorism Threat Assessment Center (STTAC), two FBI analysts, from the Western Regional Intelligence Group and the Sacramento Field Intelligence Group, were recognized for creating a product for state and local partners.
- In November 2011, a Management and Program Analyst in the Directorate of Intelligence was recognized for researching and resolving definitions to facilitate the appropriate posting of FBI products to Intelligence Community databases.
- In December 2011, a Supervisory Special Agent in the DI was recognized for coordinating FBI responses for the implementation of EO 13587 regarding Information Sharing and Safeguarding.

## **Appendix A: Authorities and Governing Principles for FBI Information Sharing, Privacy and Civil Liberties (Annotated) Framework**

Privacy and civil liberties are deeply respected and vigorously protected by the FBI. Rigorous obedience to the Constitution of the United States, respect for the dignity of all those we protect, compassion, fairness, and uncompromising personal and institutional integrity are core values of the organization and are reflected in the implementation of FBI programs.

The vital role of information sharing in the protection of our national security has been recognized and embraced at all levels of our federal government. Legislation and regulations have been enacted and programs and strategies established which operationalize and mandate the principles of information sharing, all while protecting the privacy and civil liberties of United States citizens. The important legislation, directives, regulations and programs which mandate and authorize information sharing activities and protection of privacy and civil liberties are described here.

**The United States Constitution**, in particular, the Bill of Rights, especially the First Amendment relating to freedoms of speech, assembly, the press and religion, and the Fourth Amendment relating to searches and seizures and probable cause as a basis for warrants.

**The Privacy Act of 1974**, 5 U.S.C. § 552a, Public Law No. 93-579 (Dec. 31, 1974), which governs the collection, use, maintenance and dissemination of information concerning US citizens and aliens lawfully admitted for permanent residence by the FBI and other federal agencies. The Act restricts what agencies can do with personally identifiable information in the absence of consent of the individual to whom the information pertains and imposes rules on agencies to be transparent about what information they collect and why.

FBI records are largely exempt from the access and amendment provisions of the Privacy Act because of their nature, but as a matter of discretion, the FBI may permit one-page statements of disagreement with facts found in records to be submitted by the record holder. This process is described in 28 C.F.R. 16.46(d).

**The Freedom of Information Act (FOIA)**, Public Law 89-554, 80 Stat. 383 (September 6, 1966; Amended 1996, 2002, 2007); which offers transparency of government operations by allowing any individual to request government records and to receive them, subject to applicable statutory exemptions.

Since FBI records are largely exempt from the access and amendment provisions of the Privacy Act, most individuals obtain access to FBI information through the FOIA.

**Section 208 of the E-Government Act of 2002**, Public Law 107-347347, 44 U.S.C. Ch 36 (December 17, 2002), as amended, which requires agencies to analyze privacy protections when developing information technology systems involving information in identifiable form and to prepare Privacy Impact Assessments explaining privacy risks and their mitigation.

As a matter of DOJ policy, FBI conducts PIAs on all IT systems, despite the fact that national security systems are exempt from this requirement and a significant number of our systems qualify as national security systems.

**Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004**, Public Law 108-458 (December 17, 2004), applied the lessons of the September 11 attacks to reform the IC and the intelligence and intelligence-related activities of the United States Government. Among other things, the Act established the position of DNI, the NCTC, the Privacy and Civil Liberties Oversight Board, and required the President to establish an Information Sharing Environment (ISE).

In 2007, Section 1016 of IRTPA was amended to include homeland security information as part of the ISE and weapons of mass destruction information within the definition of “terrorism.” It codifies many of the recommendations developed in response to the President’s information sharing guidelines, such as the creation of the ITACG and the development of a national network of state and major urban area fusion centers.

The ISE is defined in the Act as “an approach that facilitates the sharing of terrorism and homeland security information, which approach may include any methods determined necessary and appropriate for carrying out this section.” Its principal goal is to enable and encourage the sharing of terrorism information in a manner consistent with national security and applicable legal standards relating to privacy and civil liberties. In practice, the ISE leverages existing capabilities by adjusting and integrating current policies, business processes, standards, and systems in order to improve information sharing among all ISE participants. The authors of IRTPA carefully avoided calling the ISE a “system” or “information sharing network.” The term “environment” was used to describe a virtual infrastructure or framework which enhances and streamlines information sharing in the IC.

The IRTPA also required that the ISE incorporate protections for individuals' privacy and civil liberties. The PM-ISE developed guidelines in 2006, the *Guidelines to Ensure that the Information Privacy and other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment*” and in 2010, DOJ issued its implementation guidelines, the “*DOJ Privacy, Civil Rights and Civil Liberties Protections Policy for the Information Sharing Environment.*” The FBI adheres to IRTPA and to these implementation policies through our internal policies that protect privacy in the ISE.

**Foreign Intelligence Surveillance Act of 1978 (FISA)**, Public Law 95-511, 92 Stat. 1783, 50 U.S.C. §§ 1801 Et Seq. (October 25, 1978), as amended, which, among other provisions, establishes a separate court to oversee the collection of foreign intelligence information via electronic surveillance and provides specific protections for US person information.

**Executive Order 12333, United States Intelligence Activities** (December 4, 1981), as amended, which governs intelligence collection activities and which states that “[t]he United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms,

civil liberties, and privacy rights guaranteed by Federal law.” This Executive Order sets out the responsibilities for all members of the Intelligence Community, including the FBI.

**Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans** (October 25, 2005), superseded Executive Order 13356, which encouraged the sharing of terrorism information but only in a way that protects freedom and information privacy rights of Americans. Executive Order 13388 requires agencies to give the highest priority to the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America; and to share terrorism information with all federal, state, local, tribal and private partners, but to do so in a way that protects the freedom, information privacy, and other legal rights of Americans.

**Attorney General Guidelines for Domestic Operations (AGG-DOM)**, which recognize importance of conducting all activities in "a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people." These Guidelines are issued under the authority of the Attorney General as provided in sections 509, 510, 533, and 534 of title 28, United States Code, and Executive Order 12333. They apply to domestic investigative activities of the FBI and are enforced through FBI and DOJ oversight.

**FBI Policy for Protecting Privacy in the Information Sharing Environment**, which states that the FBI will share terrorism information, as defined in section 1016 of the IRTPA (codified at 6 U.S.C.A. Section 485), according to law, Executive Orders, Department of Justice and FBI policy, Office of the Director of National Intelligence Directives, mission justification, and the lawful authority of the requester and in a manner that protects the privacy, civil liberties, and other legal rights of US people.

**Domestic Investigations and Operations Guide (DIOG)**, which expands upon this privacy and civil liberties policy statement, weaving respect for privacy and civil liberties throughout the manual and making them an integral part of every investigative activity. The DIOG establishes the FBI’s internal rules and procedures to implement the Attorney General’s Guidelines for Domestic FBI Operations and is enforced through internal FBI oversight, as well as review by DOJ. For example, the FBI Office of Integrity and Compliance (OIC) develops, implements, and oversees a program to ensure strict compliance with all applicable laws, regulations, rules and policies. Program managers in OIC must proactively identify legal risks and implement plans to mitigate them.

**Strong oversight by the Department of Justice, the Executive Branch, Congress and the courts:**

- Intelligence Oversight Board (IOB) - reports violations of statutes, executive orders, presidential directives, and regulations and other significant or highly sensitive matters to the President
- Department of Justice – National Security Division (NSD) – conducts National Security Reviews for compliance with AG Guidelines and Minimization reviews for compliance with minimization procedures

- Department of Justice – Office of the Inspector General (OIG) - Conducts internal investigations of suspected violations of law and internal regulations
- FISA Court - approves minimization procedures adopted by the Attorney General
- Legislative Oversight: Senate and House Select Committees on Intelligence; Senate and House Judiciary Committees

**Intelligence Community Directive 501**, “Discovery and Dissemination or Retrieval of Information Within the Intelligence Community,” was issued by the DNI and became effective on January 21, 2009. This directive charges each agency in the IC with a “responsibility to provide” information, thereby ensuring agencies can “discover” and “request” intelligence from each other in order to fulfill their respective missions. ICD 501 does not apply to purely law enforcement information. If, however, it contains intelligence-related information, that information is subject to ICD 501. In order to facilitate the efficient sharing of this information, members of the IC, including the FBI, must make all intelligence and analysis available to each other by automated means. Although there remain ways to withhold information in limited circumstances, authorized IC members who request intelligence will be presumed to have a “need to know.” To withhold information, an IC element must show that sharing will jeopardize the protection of sources, methods or activities, compromise a criminal or national security investigation, or be inconsistent with the law. The ODNI has defined standards and information technology architecture requirements that all IC elements must follow to perform this process. The IC Information Sharing Executive will develop, in consultation with IC elements, including the FBI, integrated implementation plans that set forth the required benchmarks each IC element must meet in order to achieve ICD 501 policy objectives.

**Law Enforcement Information Sharing Program.** The DOJ established the Law Enforcement Information Sharing Program (LEISP) to achieve the Department’s vision of creating relationships and methods for routinely and securely sharing criminal information across jurisdictional boundaries. It mandates the kind of wide-reaching information sharing program necessary to deter terrorism and to increase the amount of information available for the investigation and prosecution of criminal activity. The LEISP was designed in response to IRTPA requirements and Attorney General mandates for sharing DOJ data with the ISE.

The LEISP requires all DOJ components to share law enforcement information—unclassified and classified—with all law enforcement partners, with the exception of certain categories of information designated by the Deputy Attorney General (DAG). It minimizes barriers to information sharing, provides a single point of contact for DOJ information, and provides a foundation for information sharing among law enforcement at the federal, state, local, and tribal levels.

To advance and support the LEISP strategy, the DAG directed the FBI and other DOJ components to participate in regional and national law enforcement information sharing initiatives.<sup>2</sup> Accordingly, the FBI has implemented information sharing technologies which support this directive and which operationalize the FBI’s National Information Sharing Strategy. The Law Enforcement N-DEx)program is a national information sharing system designed for use

<sup>2</sup> See Document Library: Deputy Attorney General, Paul J. McNulty, Memorandum, "Law Enforcement Information Sharing Policy Statement and Directives" 21 December 2006.

by all federal, state, local, and tribal law enforcement agencies. N-DEx allows agencies to search and analyze data using powerful automated capabilities. It will soon incorporate OneDOJ, an alliance of law enforcement systems, to create a single, unified resource for information sharing services. OneDOJ allows information sharing among the DOJ's law enforcement components—the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); the Bureau of Prisons (BOP); the Drug Enforcement Agency (DEA); the FBI; and the US Marshals Service (USMS)—and regional law enforcement agency partners. More information on this merged capability is presented in the N-DEx section.

**FBI National Information Sharing Strategy.** The NISS is the FBI's strategy for information sharing. It provides the common vision, goals, and framework to guide FBI information sharing initiatives. The NISS complies with both the Attorney General and the DNI guidelines for information sharing and seeks to balance the "responsibility to provide" with the need to protect sources, investigative operations, national security information, and the civil liberties of US Persons.

The NISS has two primary objectives: 1) to create and sustain a culture of information sharing, and 2) to develop and maintain an IT infrastructure that enables a broad spectrum of standards-based information sharing activities. The NISS identifies specific customer sets for these information sharing activities: internal FBI; Executive Branch; federal departments and agencies; state, local, and tribal entities; private sector; and foreign partners.

## **Appendix B: Description of FBI Finished Intelligence Products**

Intelligence Assessments (IAs): IAs<sup>3</sup> are intended to convey analytic conclusions about an issue or threat based on a comprehensive analysis of all available information, usually from multiple and open sources. They are tailored to the needs of intelligence consumers and are intended to be relevant, timely, and forward-looking. IAs address issues and identify implications and potential alternative outcomes or explanations to help the user formulate a course of action. IAs range from seven to ten pages in length and are approved for dissemination by the Section Chief in the relevant FBIHQ DI Analytical Section.

Intelligence Bulletins (IBs): IBs highlight new developments or trends. They are more limited in focus and depth than IAs, but as finished intelligence products go beyond reporting raw information. They create context for the new information and may offer an analytic judgment regarding its importance and impact. IBs are generally one to three pages in length, and like IAs, are approved for dissemination by the Section Chief in the relevant DI Analytical Section.

Intelligence Studies (ISs): ISs are comprehensive analytical works intended to convey conclusions about issues or threats that are based on comprehensive analyses of all available information, generally from multiple sources.

Intelligence Notes (INs): INs are operational vehicles used to convey tactical or operational intelligence between investigative and case support/case management entities, and are not intended for dissemination outside the FBI.

Intelligence Memorandums (IMs): IMs are text-based briefing or information-sharing products, generally for senior management officials. To achieve brevity, much of the underlying reporting and analysis in the memos are condensed to provide the audience with an essential understanding of the threats, as well as the actions proposed or actions already taken by the FBI to counter such threats.

Special Event Threat Assessments (SETAs): SETAs are a specific type of intelligence assessment designed to inform law enforcement and security planners of potential threats to an event, its venue, or its participants. Events are assigned ratings according to the Special Event Assessment Rating (SEAR) scale.

Intelligence Information Reports (IIRs): IIRs are the mechanism through which raw intelligence is shared within the FBI and throughout the intelligence and law enforcement communities. They are also the primary means by which the ODNI monitors and measures the FBI's intelligence reporting performance. 'Raw intelligence' refers to unevaluated intelligence information, generally from a single source, which has not been fully evaluated, integrated with other information, or interpreted and analyzed. The FBI produces IIRs across the counterintelligence, counterterrorism, criminal intelligence, cyber, and weapons of mass destruction programs.

<sup>3</sup> Intelligence Assessments serve a different purpose and are distinct from *investigative* activities called Assessments; see the FBI Domestic Investigations and Operations Guide (DIOG), section 5.

The intelligence in IIRs must be new, detailed, authoritative, and of interest. IIRs must also respect the right of US persons to participate in constitutionally protected activities. They may not be based solely on the exercise of First Amendment protected activities, or on the race, ethnicity, national origin, or religion of the subject. Threats should be reported via IIR only if the information is sufficiently detailed and reliable to serve as a basis for preventive action. IIRs must conform to these specifications:

- *New*: The information contained in the IIR must not have been previously reported by the same source, open source, or be well-known and assumed as fact by the Intelligence or Law Enforcement Communities;
- *Detailed*: The IIR should answer who, what, where, when, why, and how events in the IIR were attributed to or occurred. All six need not necessarily be included, but the totality of information should provide recipients with enough information to actually use the intelligence (i.e. it should be actionable);
- *Authoritative*: An IIR is authoritative if its source (or sources) could credibly have access to the information presented. The source's access need not be confirmed, but the standard is whether the source could be in a position to have learned the intelligence that the IIR contains;
- *Of Interest*: The IIR must address at least one FBI National or Field Office Collection Requirement; and
- *US Persons*: Any US Person named in the IIR should meet the following standards:
  - The FBI has an open investigation on the individual or there is an indication or allegation that the person has engaged (or will engage) in criminal activity or a poses a threat to national security;
  - The IIR would be devoid of analytic/actionable value if the name were excluded and the IIR will assist the recipient agency in conducting a lawful criminal or intelligence investigation or will assist the recipient agency in the performance of any of its authorized functions.

Tearlines: A tearline is the area in a raw or finished intelligence product where selected information of a more highly classified and/or controlled report is removed and/or sanitized to enable broader dissemination of the product at various classification levels. The remaining material contains the substance of the original intelligence without identifying sensitive sources and methods. Intelligence Community Guidance requires the FBI to provide intelligence at multiple security levels appropriate to the security authorizations of the intended recipients, and tearlines are one method to accomplish this. The following topics would be suitable for tearline dissemination:

- Imminent threats to state, tribal, or local personnel or jurisdictions;
- Potential targets of terrorism within foreign, state, tribal, or local jurisdictions;
- Activities, financing, and capabilities of terrorist or criminal organizations; and
- Collaboration among terrorist or criminal organizations.

Situational Information Reports (SIRs): SIRs are vehicles for field offices to share locally derived information on criminal or domestic terrorism matters that are relevant or of interest to only entities within their domain, such as state, local, and tribal law enforcement partners. Because the information is typically operational in nature and actionable by or relevant to only a limited audience in specific domains, it usually does not meet the same criteria that the FBI has established for intelligence products such as IIRs, IBs, ISs, or IAs.

## Appendix C: Acronyms

AAT	Advanced Analysis and Tools Cell
ACS	Automated Case Support System
AGG-DOM	Attorney General Guidelines for Domestic Operations
APG	Access Policy Group
A-Space	Analytic Space
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BOP	Bureau of Prisons
CDC	Chief Division Counsel
CICC	Criminal Intelligence Coordinating Council
CISO	Chief Information Sharing Officer
CJIS	Criminal Justice Information Services
COI	Community of Interest
CSG	Counterterrorism Steering Group
CTMIX	Community Terrorism Metadata Index
CUI	Controlled Unclassified Information
DAG	Deputy Attorney General
DaLAS	Data Loading and Analysis System
DEA	Drug Enforcement Agency
DHS	Department of Homeland Security
DI	Directorate of Intelligence
DIDO	Designated Intelligence Disclosure Official
DIOG	Domestic Investigations and Operations Guide
DNI	Director of National Intelligence
DOD	Department of Defense
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FBIHQ	FBI Headquarters
FDM	Foreign Dissemination Manual
FDO	FBI Foreign Disclosure Officer
FIG	Field Intelligence Group
FISA	Foreign Intelligence Surveillance Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FPAG	Federal Private Alliance Group
HSDN	Homeland Secure Data Network
HSPD	Homeland Security Presidential Directive
IA	Intelligence Assessment
IAFIS	Integrated Automated Fingerprint Identification System
IB	Intelligence Bulletin
IC	Intelligence Community
ICD	Intelligence Community Directive
IC ISSC	Intelligence Community Information Sharing Steering Committee

IDW	Integrated Data Warehouse
IIR	Intelligence Information Report
IOB	Intelligence Oversight Board
IOC	International Organized Crime
IM	Intelligence Memorandum
IN	Intelligence Note
IPM/ASAC	Intelligence Program Manager/Assistant Special Agent in Charge
IS	Intelligence Study
ISA IPC	Information Sharing and Access Interagency Policy Committee
ISC	Information Sharing Council
ISE	Information Sharing Environment
ISPB	Information Sharing Policy Board
ISPG	Information Sharing Policy Group
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
IST	Information Sharing Team
ITACG	Interagency Threat Assessment Coordination Group
JTTF	Joint Terrorism Task Forces
JWICS	Joint Worldwide Intelligence Communications System
LCC	LEISP Coordinating Committee
LEA	Law Enforcement Agency
LEGAT	Legal Attaché
LEISP	Law Enforcement Information Sharing Program
LEO	Law Enforcement Online
LES	Law Enforcement Sensitive
LNI	Library of National Intelligence
MLAT	Mutual Legal Assistance Treaties
MOU	Memorandum of Understanding
NCTC	National Counterterrorism Center
N-DEx	Law Enforcement National Data Exchange
NCIC	National Crime Information Center
NGIC	National Gang Intelligence Center
NIS	National Intelligence Strategy
NISS	National Information Sharing Strategy
NJTTF	National Joint Terrorism Task Force
NSB	National Security Branch
NSC	National Security Council
NSD	National Security Division
NSI	Nationwide SAR Initiative
NSIS	National Strategy for Information Sharing
OCDETF	Organized Crime Drug Enforcement Task Force
ODNI	Office of the Director of National Intelligence
OFC	Organized Crime Drug Enforcement Task Force Fusion Center
OIG	Office of the Inspector General
PII	Personal Identifying Information
POC	Point of Contact
PM-ISE	Program Manager - Information Sharing Environment

PMO	Program Management Office
PSU	Production Services Unit
SAR	Suspicious Activity Reporting
SAR	System Access Request
SBU	Sensitive but Unclassified Information
SCI	Sensitive Compartmented Information
SEAR	Special Event Assessment Rating
SETA	Special Event Threat Assessment
SIG	Special Interest Group
SIPRNET	Secret Internet Protocol Router Network
SIR	Situational Information Report
TIDE	Terrorist Identities Datamart Environment
USC	United States Code
USMS	United States Marshals Service
VGTOF	Violent Gang and Terrorist Organizations File
VPN	Virtual Private Network