

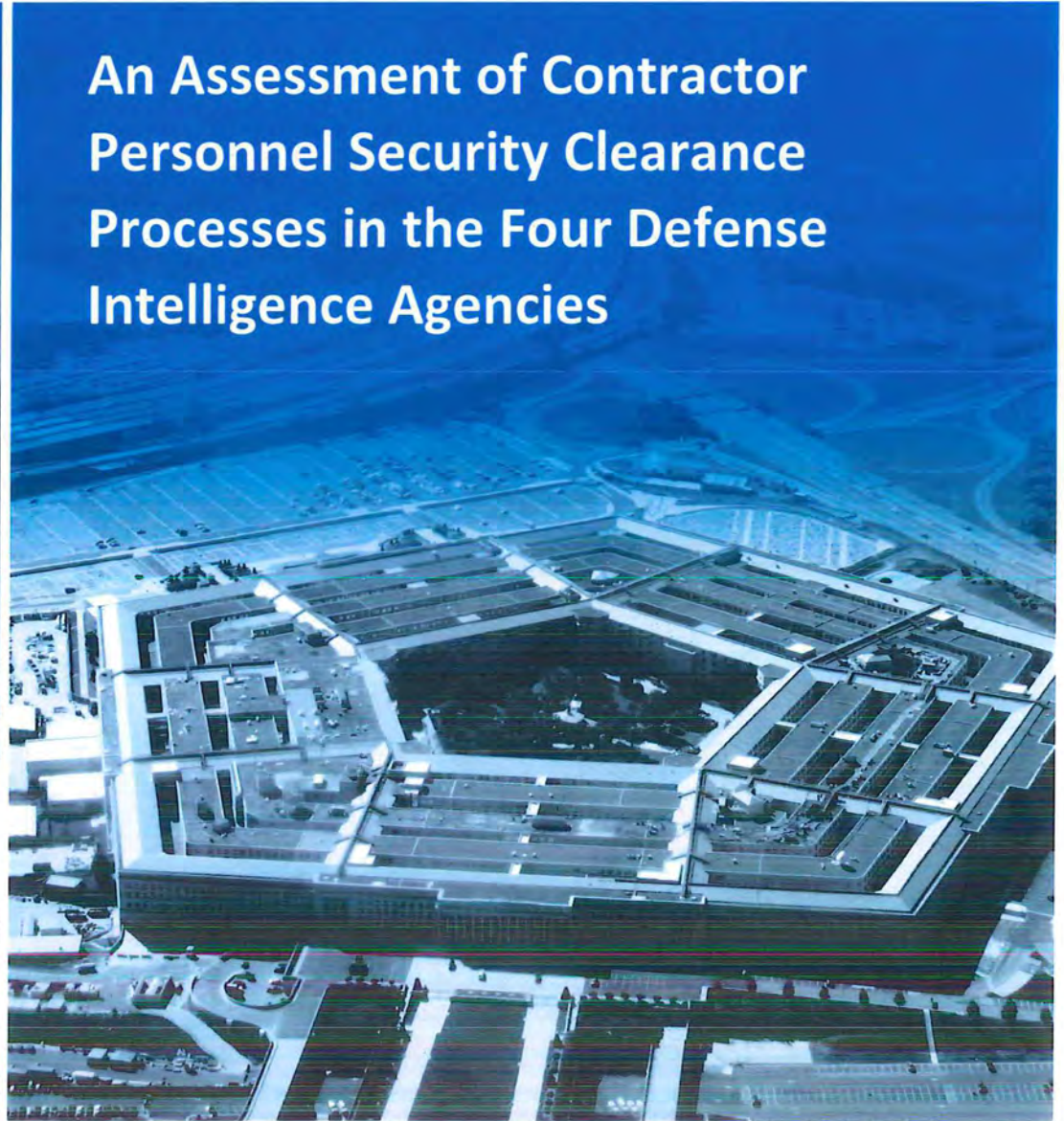


# INSPECTOR GENERAL

*U.S. Department of Defense*

April 14, 2014

## An Assessment of Contractor Personnel Security Clearance Processes in the Four Defense Intelligence Agencies



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

### **Mission**

*Our mission is to provide independent, relevant, and timely oversight of the Department that: supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.*

### **Vision**

*Our vision is to be a model oversight organization in the federal government by leading change, speaking truth, and promoting excellence; a diverse organization, working together as one professional team, recognized as leaders in our field.*

.....  
Fraud, Waste and Abuse  
**HOTLINE**  
1.800.424.9098 • [www.dodig.mil/hotline](http://www.dodig.mil/hotline)  
.....

For more information about the whistleblower protection, please see the inside back cover.



INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
4800 MARK CENTER DRIVE  
ALEXANDRIA, VIRGINIA 22350-1500

April 14, 2014

MEMORANDUM FOR: UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE  
GENERAL COUNSEL, DEPARTMENT OF DEFENSE  
DIRECTOR, DEFENSE INTELLIGENCE AGENCY  
DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY  
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE  
DIRECTOR, NATIONAL SECURITY AGENCY  
DIRECTOR, DEFENSE HUMAN RESOURCES ACTIVITY


SUBJECT: An Assessment of Contractor Personnel Security Clearance Processes in the  
Four Defense Intelligence Agencies (Report No. DODIG-2014-060)

We are providing this report for your review and comment. We considered management comments on a draft of the report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. Please see the recommendations table at page v. We request that the Office of the Under Secretary of Defense for Intelligence provide us with documentation regarding the milestones discussed in its comments. Recommendation A.3. has been redirected to the Office of the General Counsel (OGC), Department of Defense. Request that OGC respond to Recommendation A.3. within 30 days from the date of this report. Request that Director, Defense Intelligence Agency, and Director, National Reconnaissance Office, provide a response to Recommendation B.2.c. within 30 days from the date of this report.

Request that you send your responses in electronic format (Adobe Acrobat file only) to [donald.dixon@dodig.mil](mailto:donald.dixon@dodig.mil). Copies of your responses must have the actual signature of the authorizing official for your organization. We are unable to accept the /Signed/ symbol in place of the actual signature. Classified electronic format comments must be sent via the Joint Worldwide Intelligence Communications System (JWICS) to [igdixde@dodig.ic.gov](mailto:igdixde@dodig.ic.gov), or over the SECRET Internet Protocol Router Network (SIPRNET) to [donald.dixon@dodig.smil.mil](mailto:donald.dixon@dodig.smil.mil).

We appreciate the courtesies extended to our staff. Please direct questions to me at (703) 822-4860, DSN 499-7234, [REDACTED]

  
Anthony C. Thomas  
Deputy Inspector General  
for Intelligence and Special  
Program Assessments

(U) THIS PAGE INTENTIONALLY LEFT BLANK



# Results in Brief

## *An Assessment of Contractor Personnel Security Clearance Processes in the Four Defense Intelligence Agencies*

April 14, 2014

### What We Did

Our objective was to assess: a) how, or if, substantiated investigations of misconduct were reported to Agency Clearance Adjudication Facilities (CAF) and to the DoD Consolidated Adjudication Facility (DODCAF); b) if the referred investigations had been adjudicated; and c) the results of those security adjudications.

### What We Found

- There was a lack of effective personnel security policy.
- There was a lack of effective record keeping.
- There was an avoidance of personnel security adjudication for contractor personnel involved in misconduct.
- There was a lack of personnel security information sharing.
- There was a lack of connectivity between the Defense Central Index of Investigations (DCII) and the Joint Personnel Adjudicative System (JPAS).

### Our Recommendations and Management Responses

We recommend that the Under Secretary of Defense for Intelligence [USD(I)]: develop overarching policies governing operation of DCII and JPAS; expedite publishing new security policy; and advocate revising EO 12968 to require that personnel security clearance adjudicative and due process actions continue, even if the contractor employee no longer has access to classified information. USD(I) concurred with these recommendations. We redirected revision of one directive to Office of General Counsel, DoD.

We recommend that the Offices of Security of the Defense Intelligence Agency (DIA), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), and National Security Agency (NSA), Offices of Security, develop formal procedures to ensure that reports of investigation into misconduct by contractor personnel are reported to the appropriate adjudicative organizations; and ensure that the appropriate security databases are populated with personnel security adjudicative determinations. The Agencies concurred with some of these recommendations and non-concurred with others. (See the report and Appendices D – G).

We recommend that the Directors of DIA, NGA, NRO, and NSA ensure IG reports of investigation into contractor misconduct are reported to DODCAF. The Agencies concurred with this recommendation.

Lastly, we recommend that the Director, Defense Human Resources Activity (DHRA), (1) work with the General Services Administration to add the Excluded Parties List System/System for Award Management to the set of databases accessed by the Automated Continuing Evaluation System that the Defense Personnel Security Research Center developed; and, (2) develop software to automatically flag the personnel security adjudicative portion of JPAS that a DCII file exists on a specific Subject. The Defense Manpower Data Center manages both JPAS and DCII. DHRA did not concur with action 1, but did concur with action 2.

Visit us on the web at [www.DoDig.mil](http://www.DoDig.mil)

## Recommendations Table

Management	Recommendation(s) Requiring Additional Comments	Date Comments Requested	Recommendations Requiring No Additional Comments
Under Secretary of Defense for Intelligence [USD(I)]	B.1.a.	October 15, 2014	A.1., A.2., B.1.c., and C.
USD(I)	B.1.b.	May 1, 2014	
USD(I)	B.1.d.	July 15, 2014	
General Counsel, Department of Defense	A.3.	May 14, 2014	
Director, Defense Intelligence Agency	B.2.c.	May 14, 2014	B.2.a., B.2.b., and B.3.
Director, National Geospatial-Intelligence Agency			B.2.a., B.2.b., B.2.c., and B.3.
Director, National Reconnaissance Office	B.2.a., and B.2.c.	May 14, 2014	B.2.b. and B.3.
Director, National Security Agency	B.2.a.	May 14, 2014	B.2.b., B.2.c., and B.3.
Director, Defense Human Resources Activity	B.4.	May 14, 2014	E.
Inspector General, Defense Intelligence Agency			B.3
Inspector General, National Geospatial-Intelligence Agency			B.3.
Inspector General, National Reconnaissance Office			B.3.
Inspector General, National Security Agency			B.3.

*Distribution:*

Secretary of Defense  
Deputy Secretary of Defense  
Under Secretary of Defense for Personnel and Readiness  
Assistant to the Secretary of Defense for Intelligence Oversight  
Director, Office of Cost Assessment and Program Evaluation, OSD  
Chairman, Senate Select Committee on Intelligence  
Chairman, House Permanent Select Committee on Intelligence  
Chairman, Senate Armed Service Committee  
Chairman, House Armed Services Committee  
Chairman, Senate Committee on Homeland Security and Governmental Affairs  
Director of National Intelligence  
Inspector General of the Intelligence Community  
Director, Special Security Directorate, Office of the National Counterintelligence  
Executive/Security  
Director, Office of Security, Central Intelligence Agency  
Director, Office of Management and Budget  
Deputy Director for Management, Office of Management and Budget  
Director, Office of Personnel Management  
Director, Federal Investigation Services, Office of Personnel Management  
Archivist of the United States  
Director, Defense Security Service  
Inspector General, Defense Security Service  
Chair, Council of the Inspectors General on Integrity and Efficiency  
Inspector General, Defense Intelligence Agency  
Director, Office of Security, Defense Intelligence Agency  
Inspector General, National Geospatial-Intelligence Agency  
Director, Office of Security, National Geospatial-Intelligence Agency  
Inspector General, National Reconnaissance Office  
Director, Office of Security, National Reconnaissance Office  
Inspector General, National Security Agency  
Director, Office of Security, National Security Agency  
Director, Department of Defense Consolidated Adjudication Facility

# Contents

---

Introduction.....	1
Background.....	1
Objectives.....	1
Scope and Methodology.....	1
Finding A. Lack of Effective Personnel Security Policy.....	2
Finding B. Lack of Effective Recordkeeping.....	7
Finding C. Avoidance of Personnel Security Adjudication and Due Process Issues.....	24
Finding D. Lack of Personnel Security Information Sharing.....	27
Finding E. Lack of Connectivity Between DCII and JPAS.....	30
Other Observation.....	32
Appendix A. Background.....	33
Appendix B. Scope and Methodology.....	35
Appendix C. Office of the Under Secretary of Defense for Intelligence Response.....	37
Appendix D. Defense Intelligence Agency Response.....	40
Appendix E. National Geospatial-Intelligence Agency Response.....	42
Appendix F. National Reconnaissance Agency Response.....	44
Appendix G. National Security Agency Response.....	47
Appendix H. Defense Human Resources Activity Response.....	50
Acronyms and Abbreviations.....	52



# Introduction

---

## Background

On September 5, 2012, we published the memorandum report, *The Four Defense Intelligence Agencies Have Had No Effective Procedures for Suspension and Debarment*. That project's objective was to determine the effectiveness of suspension and debarment procedures in the four Defense intelligence agencies -- the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and the National Security Agency (NSA). We based our study on 131 investigative case summaries (hereinafter referred to as "IG investigations") provided to us by the Inspectors General (IGs) of the Defense intelligence agencies from October 1, 2000, to September 30, 2010; we published those case summaries in the *Classified Annexes to the [DoD IG's] Semi-Annual Report to Congress*. In our study, we found that none of these Agencies had ever debarred a contractor, consultant, or contractor employee. Also, we found that only one of these agencies had ever suspended a contractor, consultant, or contractor employee.

During our research for that project, we found that procurement and general counsel staff from the Defense intelligence agencies had assumed that Subject contractor employees involved in misconduct would lose their security clearance and access. We examined this assumption using the same 131 cases that we had used in the suspension and debarment study. Also in our research we determined that absent suspension and debarment there was no policy to preclude individuals involved in misconduct investigated by Agency IGs from working on unclassified government contracts, even if they had lost their security clearance and Sensitive Compartmented Information (SCI) access. A detailed discussion of the background to this project is attached as Appendix A.

## Objectives

In response to our initial data call to the IGs of the Defense intelligence agencies, the IGs identified 128 individuals as the Subjects of their 131 substantiated investigations. Although these investigations were conducted by the Agency IGs between 2000 and 2010, we conducted our research to determine if they were still relevant to contractor personnel security clearance processing in the Department. The extent to which they impacted individual personnel security adjudicative decisions was within the scope of authority of the individual Agency Directors and Agency Clearance Adjudication Facilities (CAF). We assessed: a) how, or if, substantiated investigations of misconduct were reported to their Agency CAF and to the Department of Defense (DoD) Consolidated Adjudication Facility (DODCAF); b) if the referred investigations had been adjudicated; and c) the results of those security adjudications. DODCAF is the successor organization to the Defense Industrial Security Clearance Office (DISCO); the U.S. Army, U. S. Navy, U.S. Air Force, Washington Headquarters Services, and Joint Staff CAFs, and for the adjudicative functions of the Defense Office of Hearings and Appeals (DOHA).

## Scope and Methodology

A detailed discussion of our scope and methodology is attached as Appendix B.

## Finding A

---

### Lack of Effective Personnel Security Policy

We found a lack of effective personnel security policy. This condition occurred because the Department's personnel security policy was largely outdated, or -- as in the case of policy for operation of the Joint Personnel Adjudication System (JPAS) -- entirely absent. As a result, a lack of effective security policy procedures existed, with no overarching written policy governing how/when JPAS is to be used.

### Applicable Personnel Security Policy

We conducted a detailed review of personnel security policy, including Executive Orders (EO); Intelligence Community (IC) policy issued by the Director of National Intelligence (DNI); Office of Personnel Management (OPM)-issued policy; and DoD-issued policy. Based on our review, we found:

- Many of the 131 Agency IG case summaries included misconduct, which warranted either: a) additional conditions, deviations, or waivers attached to a favorable security clearance/access adjudication; or b) revocation/denial of one's security clearance/access.
- Under the reciprocity policy of Intelligence Community Policy Guidance (ICPG) 704.4, "Reciprocity of Personnel Security Clearance and Access Determinations," a favorable personnel security clearance/SCI access adjudicative determination -- absent conditions, deviations, or waivers -- made by one CAF was binding on all other IC elements.
- Defense intelligence agencies were required to report unfavorable information regarding contractor employees to DISCO, and now to DODCAF.

### Outdated Personnel Security Policy Documents

DoD Instruction (DoDI) 5025.01, "DoD Directives Program," September 26, 2012, established that "Prior to the 5-year anniversary of their publication date, all issuances must be reviewed to determine if they are necessary, current and consistent with DoD policy, existing law, and statutory authority. They will be either reissued, certified as current, or cancelled, as appropriate...All issuances certified as current must be reissued or cancelled within 7 years of the original publication date."

The DoD personnel security policy documents we reviewed were between eight and 28 years old. None of them met the standards of DoDI 5025.01 for accuracy and currency. Among the many problems we noted were:

- Repeated references to the Defense Investigative Service (DIS), which was renamed the Defense Security Service (DSS) in 1997.
- The documents did not reflect the transfer in February 2005 of the DoD personnel security background investigative mission from DSS to OPM.

- Repeated references to the Directorate for Industrial Security Clearance Review (DISCR), which was succeeded by the Defense Office of Hearings and Appeals (DOHA), and which has now been succeeded, in part, by DODCAF.
- The documents did not reflect the creation of JPAS, the move of personnel security investigative and adjudicative records from the Defense Clearance and Investigative Index to JPAS, and the further renaming of the Index as the Defense Central Index of Investigations (DCII).
- The numerous organizational changes since these policy documents were published make the required reporting channels difficult to understand. Of note, Commanders and heads of activities are generally required to report adverse/questionable information concerning contractor employees who are cleared, or are being cleared, for access to classified information to DISCO/DODCAF.

Also of note, USD(I) staff told us that DoD personnel security policy had been under detailed review, and in coordination since 2012.

## There is no Overarching Written Policy Governing JPAS

JPAS was designed to provide the Department with a common information resource for granting and sharing personnel security eligibility determinations and recording personnel access to sensitive and non-sensitive compartmented information. We did not find any overarching policy documents -- such as a directive, regulation, or instruction -- governing JPAS operation.

## Responsibility

DoDI 5145.03, "Oversight of the DoD Personnel Security Program," January 2013, charges the USD(I) with direction, administration, and oversight of the DoD personnel security program. Further, the February 2010 Memorandum of Agreement covering the transfer of operational control of JPAS and DCII from DSS to the Defense Manpower Data Center (DMDC) stipulated that USD(I) "retained responsibility for creation and interpretation of all policies governing" JPAS and DCII.

## Conclusions

DoD personnel security policy is dated, unclear, or entirely absent. Since no system can function in the absence of adequate direction; it is imperative that this situation be resolved as soon as possible.

## Recommendations, Management Comments, and Our Response:

**A. 1. We recommend that USD(I) develop and issue an overarching policy governing operation of the System of Record for Personnel Security Clearances.**

### USD(I) Comments

In our coordination draft, we recommend that USD(I) develop and issue an overarching policy governing JPAS operation. USD(I) concurred with the recommendation, agreeing that a consolidated, overarching policy was needed. USD(I) stated that Draft DoDM 52200.02, Volume 1, "DoD Personnel Security Program: Investigations for National Security Positions and Duties," and DoDM 5200.02, Volume 2, "DoD Personnel Security Program: Adjudications, Due Process, Continuous Evaluation and Security Education," will "provide overarching policy governing operations of JPAS and its successor system (the Joint Verification System), to include requirements for recording issues of security concern and adjudications that are based on exceptions due to presence of adverse information. Since Volume 2 is still in the formal comment period, we have an immediate opportunity to ensure that we incorporate the IG's recommendations and address the need for JPAS functionality as discussed in the IG report."

### Additional Comment by the Defense Human Resources Activity (DHRA)

DHRA recommended that the recommendation be modified to require that USD(I) develop and issue an overarching policy governing the "System of Record for Personnel Security Clearances," stating that a transition from JPAS to the Defense Information System for Security (DISS) is planned.

### Our Response

The USD(I) comments are responsive, and the additional DHRA comment is an appropriate clarification. Accordingly, we modified the recommendation.

**A.2. We recommend that USD(I) finalize updates to -- or replacements for -- the personnel security portions of the following Departmental policies:**

- a. DoD 5200.2-R, "Personnel Security Program," February 23, 1996.
- b. DoD 5220.22-R, "Industrial Security Regulation," December 1985.
- c. DoD 5220.22-M-Sup 1, "National Industrial Security Program: Operating Manual Supplement," February 1995.

### USD(I) Comments

USD(I) concurred with the recommendation, and provided the following timeline

regarding replacements for the above policy documents:

DoD 5220.2-R is being replaced by DoDM 5200.02, Vol. 1, and DoDM 5200.02, Vol. 2.

Volume 1 has been in the Office of the General Counsel, Intelligence [OGC(I)], DoD, since July 29, 2013, for legal sufficiency review. Following OGC(I) review, USD(I) will expedite making any required changes before moving the policy to Office of the General Council (OGC), DoD, for approval. Thereafter, USD(I) is required to coordinate with the Federal Register Liaison Office (FRLO), Washington Headquarters Services (WHS), which coordinates with the Office of Management and Budget (OMB) to meet OMB's requirements for publishing the policy as a federal rule.

Formal Coordination of Volume 2 closed on January 17, 2014. USD(I)'s goal is to complete adjudication of comments by March 7, 2014. Thereafter, the policy issuance process will proceed according to the steps that WHS established and according to the timelines that DoDI 5025.01 established. Once through the DoD policy issuance process, USD(I) is required to coordinate with FRLO to move the proposed policy through OMB's rule-making process.

DoD 5220.22-R will be replaced by DoD 5220.22M, Vol. 2, "National Industrial Security Program: Industrial Security Procedures for Government Activities." DoD will work with WHS who coordinates with OMB to publish the policy through OMB's Federal Register process. DoD is currently working with OMB to format the volume and to complete information collection in accordance with OMB requirements.

DoD 5220.22-M-Sup 1 will be cancelled when the next conforming change to DoD 5220.22-M is approved. That policy is currently being processed through the formal DoD policy-issuance process. USD(I)'s goal is to issue the conforming change by January 1, 2015.

USD(I) advised that despite the issuance of DoDI 5145.03, DoD OGC retained policy responsibility for DoDD 5220.6, "Defense Industrial Personnel Security Clearance Review Program," April 4, 1999.

## Our Response

The USD(I) comments are responsive.

## Redirected Recommendation

As a result of USD(I)'s comments, we are redirecting the following recommendation to DoD OGC.

**A.3. We recommend that DoD OGC prepare an update to -- or replacement for -- DoDD 5220.6 to make it compliant with the requirements of DoDI 5025.01 for accuracy and currency.**

## Finding B

### Lack of Effective Recordkeeping

We found a lack of effective recordkeeping by the Agency security offices, as well as by DIA, NGA, NRO, and NSA IGs. This occurred because the appropriate investigative and personnel security databases -- JPAS, DCII, and the IC's SCATTERED CASTLES system -- were not being reliably populated with investigative and security information. As a result, the failure to effectively document investigative Subjects in JPAS, SCATTERED CASTLES, and/or DCII significantly hindered personnel security clearance and access adjudications.

### Background

The Subjects of the investigations that the Agency IGs conducted generally had the highest levels of security clearance and access to classified material. The following table summarizes our understanding of the authorized levels of security clearance/access that the contractor employees (the Subjects) held at the time the IGs conducted their investigations:

Contractor Employee (Subjects) Security Clearance/Access						
Agency	Number of Subjects with either No or Unknown Level of Clearance/Access	Number of Subjects with Confidential	Number of Subjects with Secret	Number of Subjects with Top Secret Collateral Only	Number of Subjects with Top Secret/SCI	Number of Subjects Total
DIA	7	0	1	0	13	21
NGA	2	0	0	0	1	3
NRO	6	0	3	0	67	76
NSA	0	0	0	0	28	28
Total	15	0	4	0	109	128

Eighty-eight percent (113 of 128) of the Subjects held a documented security clearance, and 85 percent (109 of 128) had access to Top Secret/SCI information. Based on the security classification standards articulated in EO 13526, *Classified National Security Information*, December 29, 2009, Top Secret information -- if compromised -- could reasonably be expected to cause exceptionally grave damage to the national security.

### Gaps in Joint Personnel Adjudication System (JPAS) and SCATTERED CASTLES

JPAS was designed to provide the Department with a common information resource for granting and sharing personnel security eligibility determinations and recording personnel access to sensitive and non-sensitive compartmented information. SCATTERED CASTLES serves essentially the same purpose for the IC.

In our review, we found that only 73 percent (94 of 128) of the Subjects were listed in JPAS, and only 53 percent (68 of 128) were listed in SCATTERED CASTLES.

Of the Subjects listed in JPAS, only 35 percent (33 out of 94) had relevant incident reports posted in their JPAS file by their corporate security officers or the Office of Security of the Agency whose IG had conducted the investigation.

## Conditions/Deviations/Waivers Not Adequately Documented in SCATTERED CASTLES

ICPG 704.4 raises the issue of conditions, deviations, and waivers in the security clearance process. While guidelines may support security clearance/access revocation or denial, operational considerations at times might make this difficult. OPM describes these conditions as “access eligibility granted or continued with the proviso that one or more additional measures will be required, such as additional security monitoring, restrictions on access, and restrictions on an individual’s handling of classified information.” For example, for an individual who was investigated for time and attendance fraud, a “condition” might include a requirement that contractor and government management exercise significantly heightened oversight of the individual’s time, attendance, and financial claims. The fact that clearance/access was granted with conditions, deviations, or waivers should be documented in the “Exception Information” block of the Subject’s SCATTERED CASTLES file, indicating the type (condition, deviation, or waiver), and date of the exception. Such a properly documented exception would afford a second agency the opportunity to deny reciprocity under ICPG 704.4.

In our review, at least 45 percent of the Subjects (57 of 128) continued *in status* or had clearance/access *granted or restored* after the closure dates of their IG investigations. Although substantiated Agency IG investigations existed regarding these 57 Subjects, only 10 Subjects had entries in the “Exception Information” block of their SCATTERED CASTLES files by any CAFs:

Subjects’ Files in SCATTERED CASTLES Where the “Exception Information” Block Indicates Clearance/Access was Granted with a Condition, Deviation, or Waiver	
Investigating Agency	Number of Subjects with annotations indicating Condition “C”, Deviation “D,” or Exception “E”
DIA IG	1 “C” entered by NRO CAF 2 “D” entered by DIA CAF 1 “D” entered by both DIA and CIA CAFs
NGA IG	0
NRO IG	1 “D” entered by DIA CAF 1 “D” entered by NRO CAF 3 “C” and “D” entered by NRO CAF
NSA IG	1 “D” entered by CIA CAF
Total	10

The misconduct documented in the IGs’ investigative case summaries appeared to warrant referral to their Agencies’ CAF for adjudication, and referrals did occur in all 57 cases. We cannot determine from the data provided to us whether the CAFs either: a)



made the judgment that the misconduct was not of sufficient significance to warrant granting clearance/access with conditions, deviations, or waivers; or b) if clearance/access was granted with conditions, deviations, or waivers, but these exceptions were not documented by the CAFs in the Subjects' SCATTERED CASTLES files.

Without a documented condition, deviation, or waiver, a Subject would be eligible under the reciprocity policy of ICPG 704.4 for equivalent or lower access at all other IC entities.

## Gaps in the Defense Central Index of Investigations (DCII)

DCII was created in February 1966 -- under a December 3, 1965, memorandum signed by Deputy Secretary of Defense Cyrus Vance -- to constitute a computerized central index of investigations conducted by DoD investigative activities. Despite extensive efforts, we have been unable to recover a copy of Mr. Vance's memorandum to determine his intent in directing the establishment of DCII. The initial executive agent for DCII was the Office of the Assistant Chief of Staff for Intelligence, U.S. Army. Executive agency was subsequently transferred to DIS/DSS in 1972. And, in mid-2010 the Deputy Secretary of Defense transferred operational responsibility for DCII to the DMDC. From the chain of executive agency for DCII -- and the historic inclusion of personnel security background investigations, counterintelligence polygraph examinations, counterintelligence investigations, security investigations, and personnel security clearance data in DCII, as well as criminal investigative data -- it is reasonable to conclude that the database was initially broadly defined as an investigative index.

A DCII file consists of a Subject's name; social security number; date, state, and country of birth; investigative file number(s), location and year the file(s) was created; context of the Subject's relationship to the investigation (i.e., Subject, witness, cross reference, etc.), retention period of the investigative file(s); and date the investigation(s) was closed. The file contains no investigative information and simply functions as a finding guide for where DoD investigative files are located.

The majority of the 131 Agency IG investigations we reviewed involved possible violations of Federal criminal statutes. For example, time and attendance fraud -- which comprised 68 percent of our case sample (89 of 131 cases) -- generally involves some combination of violations of the following Federal criminal statutes:

- 18 U.S. Code (USC), 287, False, Fictitious, or Fraudulent Claims
- 18 USC 1001, False Official Statement
- 18 USC 1341, Mail Fraud
- 18 USC 1343, Fraud by Wire

Moreover, in order to significantly profit from time and attendance fraud, a Subject must have submitted false claims/statements during repeated payroll cycles. The time and attendance fraud investigations involved an average loss per investigation of \$41,788.96.

A possible violation of the criminal statutes is indicated when an IG refers an investigation to the Criminal and Civil Divisions of the Department of Justice (DoJ), or to local prosecutors. However, while investigations were referred for possible prosecution, they were not always titled and indexed in DCII (as shown in the following chart):

Overall Agency Totals							
Agency	Cases in Our 131 Case Sample	Duplicate Case Summaries	Exclusively Corporate Subjects (i.e., no identified individual Subjects)	Individual Subjects Identified	Cases Referred To DoJ or Local Prosecutors (based upon the 131 Case summaries)	Individual Subjects Titled and Indexed in DCII	Individual Subjects Not Titled and Indexed in DCII
DIA	20	0	4	21	3	8	13
NGA	3	0	1	3	1	0	3
NRO	80	1	5	76	72	23	53
NSA	28	1	2	28	9	12	16
Total	131	2	12	128	85	43	85

As documented in the above chart, only 34 percent of the Subjects (43 of 128) were titled and indexed in DCII. Only the Defense Criminal Investigative Service (DCIS), the law enforcement investigative arm of DoD IG -- which had worked jointly with Agency IGs on some cases -- and DIA IG titled and indexed Subjects in DCII.

We noted some anomalies during our research. While the Subjects in nine NSA IG cases were presented to Federal prosecutors for possible prosecution, five of those Subjects were not titled or indexed in DCII. Nor did corporate or Agency security officials file relevant incident reports in JPAS. Also, three of those five Subjects continued to hold SCI access with NSA, even after the NSA IG investigations concluded.

Additionally, while the Subjects in 72 NRO cases were presented to Federal prosecutors for possible prosecution, 20 were not titled or indexed in DCII, and no relevant incident reports were filed in JPAS regarding those Subjects.

We also received some anecdotal data during our review. Staff members of the NGA, NRO, and NSA IGs told us that:

- NGA IG had only recently obtained "read only" access to DCII, and was attempting to obtain "full user" access to DCII so that it could title and index Subjects in DCII. In response to our draft report, NGA advised that NGA IG had obtained full user access to DCII, effective August 26, 2013.
- NRO IG had not titled and indexed Subjects from its criminal investigations in DCII for "some years," and staff did not know if their IG still had a staff member with decisional authority to title and index Subjects in DCII. In response to our

draft report, NRO advised that NRO IG never had access to DCII and its IG investigators may have misspoken. NRO IG had relied on the NRO Office of Security and Counterintelligence to title and index Subjects of IG investigations “in the appropriate system(s) of record.”

- NSA IG worked with DCIS on “all criminal investigations.” Therefore, as a criminal investigative entity, DCIS was responsible for titling and indexing the Subject(s) in DCII. No one was designated at NSA to title and index individuals in DCII. In this context, we noted that only 43 percent of NSA IG’s Subjects (12 of 28) were titled and indexed in DCII.

## Results of Gaps in DCII Data

Personnel security investigations begin with a National Agency Check (NAC), which is defined in 32 Code of Federal Regulations (CFR) 154, Appendix A, as a scan of at least three databases: DCII; Federal Bureau of Investigation (FBI) headquarters investigative files; and FBI identification files.

A favorable NAC, local agency check, credit check, and verification of a Subject’s birth (NACLC) are the basic criteria for granting eligibility for access to Confidential and Secret information. The Single Scope Background Investigation (SSBI) expands on the NACLC by verifying employment, education, and residence, as well as interviews of the Subject and character references. Paragraph 10.a., ICPG 704.1, “Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to [SCI] and Other Controlled Access Program Information,” requires that, at a minimum, six data bases be queried as part of a NAC for SCI access. DCII is one of these databases.

OPM maintains the Security and Suitability Investigation Index (SII) and the Central Verification System (CVS). Those systems allow personnel security and suitability communities to validate the need for new investigations and share information on prior background investigations, adjudications, security clearances, and Homeland Security Presidential Directive (HSPD) 12 credential determinations. If criminal investigative files are identified through a DCII check, the file is then copied into the Subject’s background investigation and the investigation indexed in SII.

Therefore, failing to title and index investigative Subjects in DCII significantly hinders the NAC and SSBI processes. DMDC staff told us that no system impediments currently exist for providing DCII system access to additional users, which means the Defense intelligence agencies IGs should be able to access DCII.

This situation caused us to further examine the historical development of DCII. Other than references to former Deputy Secretary of Defense Vance’s memorandum, we have been unable to find an over-arching DoD policy document -- directive, regulation, instruction, or manual -- governing the operation of DCII. This has resulted in a degree of confusion regarding which investigations should be titled and indexed in DCII.

An examination of copies of the CFR published between 1978 and 2009 provides the following information regarding DCII:

“The DCII, which contains reference to investigative records created and held by the DoD components. The records indexed are primarily those prepared by the investigative agencies of the Military departments and DIS, covering criminal, fraud, counterintelligence, and personnel security information.” [32 CFR 298.4.(a), July 1, 1978; and 32 CFR 298.3.(a), July 1, 2009]

“DIS maintains the [DCII], which contains reference to investigative records created and held by DoD components. The records indexed are primarily those prepared by the investigative agencies of the DoD, covering criminal, fraud, counterintelligence, and personnel security information.” [32 CFR 298.3.(a), July 1, 1992]

DODI 5505.07, “Titling and Indexing Subjects of Criminal Investigations in the [DoD],” January 27, 2012, discusses only the titling and indexing of the Subjects of criminal investigations conducted by the Defense Criminal Investigative Organizations (DCIO).

DODI 5505.16, “Criminal Investigations by Personnel Who Are Not Assigned to a [DCIO],” May 7, 2012, applies to all DoD Components outside the DCIOs. It establishes the policy that DoD Components who employ personnel conducting criminal investigations will ensure that Subjects of criminal investigations are titled and indexed in DCII. It requires that such DoD Components will develop an automated records management and information system which is compatible with DCII. If the component does not have full DCII user access they will execute an agreement with a DCIO or other DoD law enforcement organization to meet DCII reporting requirements. If an investigation is transferred to a DCIO, then that DCIO becomes responsible for titling and indexing the Subject(s) of the investigation in DCII.

What is much less clear are the policy requirements for titling and indexing the Subjects of complaint type personnel security, counterintelligence, security violation, unauthorized disclosure, administrative, senior official, and other investigations conducted by DoD Components.

In addition to policy issues, inadequate DCII system capacity prior to mid-2006 limited the ability of the Agency IGs and other organizations to title and index Subjects in the DCII during much of DIS/DSS’s administration of the DCII. For example, DIA IG began requesting full user access to the DCII in the early 1990s, but did not receive access until the summer of 2006 when DSS expanded DCII system capacity, relieving the earlier system capacity issues. When the DIA Office of Security (SEC) commenced conducting counterintelligence polygraph examinations in the 1990s, it was several years before DSS could provide SEC with system capability to title and index the polygraph examinations in DCII, despite DoD polygraph policy which required that the examinations be titled and indexed.

## Complete DCII Recordkeeping is Critical to the Projected Shift in Reinvestigations

During a March 5, 2013, Intelligence and National Security Policy Reform Symposium, the Director, Office of Security, NRO, said that due to constrained funding, the NSA and NRO Offices of Security had suspended the conduct of periodic reinvestigations for contractor employees, and were instead concentrating on entry-level background investigations. In response to our draft report, NSA stated that it had, in fact, not suspended contractor reinvestigations. DSS -- which funded most industry background investigations and periodic reinvestigations -- announced in June 2013 that due to fiscal constraints it was suspending all industry periodic reinvestigations for the remainder of fiscal year 2013.

Additionally, substantial momentum exists toward Continuous Monitoring, Evaluation, or Observation. This concept began when the Defense Personnel Security Research Center (PERSEREC) started examining *aperiodic* reinvestigations -- in lieu of the current reinvestigations, which are supposed to occur every five years. As a result of this research, PERSEREC developed the Automated Continuing Evaluation System (ACES). PERSEREC described this system as follows:

"...These evaluations involved automated checks of security-relevant databases, such as criminal history, credit, foreign travel, and large-currency transactions. This approach would reduce security risk by detecting more cases involving issues of serious security concern and by detecting those cases earlier. Furthermore, it would substantially reduce demands on investigative resources. This would be accomplished by applying more investigative resources to the relatively small number of cases where they are needed the most and fewer resources to cases where they are needed the least. Using this approach, full-scale investigations would be triggered based on factors such as the person's level of access, the time elapsed since the last investigation, whether issues were detected in the last investigation, and the seriousness and number of new issues detected by automated checks of security-relevant databases..."

The current system requires a minimum five-year gap between investigations, even though personnel security specialists have long recognized that significant security events could affect a Subject's life between investigations. Based upon preliminary studies and field testing, the testing organizations believed ACES to be effective and substantially less expensive than the current personnel security reinvestigation system.

Movement away from traditional background investigations -- particularly the five-year periodic reinvestigation -- requires accuracy in the data searches that will replace those investigations. DCII is among the databases contained in PERSEREC's ACES set of databases.

If ACES or another continuous monitoring program is to replace periodic reviews, DoD entities must ensure the Subjects of all DoD investigations are titled and indexed in DCII. This would enable those investigations to be recovered by the CAFs holding personnel security adjudicative responsibility for civilian government employees, military personnel, and contractor employees.

In light of our earlier study on suspension and debarment, we note that ACES does not include the Excluded Parties List System (EPLS) or the follow-on System for Award Management (SAM) in the set of databases being accessed. The General Services Administration (GSA) administers EPLS/SAM, which contains the identities of individual and corporate contractor employees who have been suspended or debarred from government contracting because of misconduct or poor performance. Suspension and debarment and personnel security adjudication are closely linked, because both deal with suitability: suspension and debarment relates to the government conducting business only with responsible contractors, while personnel security adjudication relates to suitability for access to classified information.

### **Lack of Reporting to DISCO/DODCAF**

DoD 5220.22-R requires that the head of a user activity shall report to DISCO any adverse or questionable information that comes to that person's attention concerning a contractor employee who has been cleared for access to classified information, which may indicate that such access is not clearly consistent with the U.S. national interest.

Historically, sponsoring organizations would submit requests for contractor employees' security clearance determinations to DISCO. DISCO would then task the investigative entities, receive the results of the investigations, and adjudicate for collateral security clearances. Cases that contained significant derogatory information were referred to DOHA for further adjudication and, if required, due process action. When the process was favorably completed, DISCO granted the clearances. If the contractor employee subsequently required SCI access, the case was adjudicated a second time by one of the Defense intelligence agency or Military Service CAFs. This process was admittedly time-consuming.

DNI subsequently delegated authority for the entire personnel security process to the four Defense intelligence agencies for personnel falling within their security cognizance. The four agencies now can conduct background investigations and personnel security adjudications for government employees and contractor employees, for both collateral and SCI access.

We provided our list of 128 investigative Subjects to DODCAF and followed up by asking DODCAF to review its files to determine if its predecessor CAFs had received copies of the relevant investigative reports that the Agency IGs prepared. DODCAF replied that it could only positively determine whether or not it had received an IG report on 20

percent of the Subjects (26 of 128); and for those 26 Subjects, it had only received five reports -- all of them on NRO IG Subjects.

Therefore, the four Defense intelligence agencies have *not* complied with the DoD 5220.22-R requirement to report to DISCO adverse/questionable information concerning a contractor employee with access to classified information.

## Continued Focus on Existing Databases

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) required establishing a single, integrated personnel security database no later than 12 months after the law was enacted.

The Government Accountability Office (GAO) said in a report entitled, *Personnel Security Clearances: Progress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum* (GAO-11-65, November 2010), that the executive branch agencies have instead opted to focus on leveraging existing systems rather than establishing a new database, citing concerns related to privacy, security, and data ownership. Thus, it is increasingly important for existing databases to contain current and accurate personnel security data.

## Destruction of Old Personnel Security Records

National Archives and Records Administration (NARA) General Records Schedule (GRS) 18: Security and Protective Services Records, Item 22, provides for the following:

"22. Personnel Security Clearance Files.

"Personnel security clearance case files created under Office of Personnel Management procedures and regulations and related indexes maintained by the personnel security office of the employing agency.

"a. Case files documenting the processing of investigations on Federal employees or applicants for Federal employment, whether or not a security clearance is granted, and other persons, such as those performing work for a Federal agency under contract, who require an approval before having access to Government facilities or to sensitive data. These files include questionnaires, summaries of reports prepared by the investigating agency, and other records reflecting the processing of the investigation and the status of the clearance, exclusive of copies of investigative reports furnished by the investigating agency.

"Destroy upon notification of death or not later than 5 years after separation or transfer of employee or not later than 5 years after contract relationship expires, whichever is applicable (Nc1-GRS-80-1 item 23a)

"c. Index to the Personnel Security Cases Files.

"Destroy with related case file. (NC1-GRS-80-1 item 23c)"

Throughout our review, we tried to determine: a) if a CAF had received a copy of one of the Agency IG's reports of investigation; b) if the information contained in the investigation had been adjudicated; and c) the results of the adjudication. However, our efforts were stymied because adjudicative files and indices had been destroyed in accordance with NARA GRS 18. When the Agency IG's investigative Subjects are not titled and indexed in DCII and personnel security records are also destroyed, it (inaccurately) appears as if no investigation was ever conducted. However, NARA is not within our oversight purview.

## Conclusions

If the personnel security system is to function properly, it is imperative that the appropriate investigative and security databases be populated with accurate and complete information by every entity – investigative and security – which has had an equity in the investigative/security Subject. It is clear from our evaluation that this has not been occurring consistently.

## Recommendations, Management Comments, and Our Response

**B.1.a. We recommend that USD(I) prepare an overarching policy governing the operation of DCII, including identification of the categories of investigations to be titled and indexed, and the retention criteria for investigations so titled and indexed.**

### USD(I) Comments

USD(I) concurred with the recommendation. It will convene a working group to develop, as appropriate, overarching policy governing the operation of DCII by September 30, 2014.

### Our Response

The USD(I) comment is responsive. We request that USD(I) provide us with a copy of this policy by October 15, 2014.

**B.1.b. We recommend that USD(I) direct the Defense intelligence agencies to review the procedures that their Offices of Security use to ensure that JPAS and SCATTERED CASTLES are being properly populated.**

### USD(I) Comments

USD(I) concurred with the recommendation, and will issue a memorandum directing the recommended review by April 15, 2014.



## Our Response

The USD(I) comment is responsive. We request that USD(I) provide us with a copy of the memorandum by May 1, 2014.

**B.1.c. We recommend that USD(I) direct the Defense intelligence agencies to ensure that the Subjects of Agency IG criminal investigations are titled and indexed in DCII in accordance with DoDI 5505.16.**

## USD(I) Comments

USD(I) concurred with the recommendation, stating that it would work with DoD IG “to determine the correct authorities for issuing such a requirement.”

## Our Response

The USD(I) comment is responsive. However, we believe that for the present time, DoDI 5505.16 provides adequate authority to support this recommendation. It may be appropriate in the future to meld the provisions of DoDI 5505.16 and DoDI 5505.07 into the overarching DCII policy that was discussed in Recommendation B.1.a.

**B.1.d. We recommend that USD(I) conduct one of the following actions to ensure Subjects of past investigations are titled and indexed in DCII:**

- **Initiate action with OPM to require that OPM investigators conducting background investigations on current and former civilian employees, military assignees, and contract employees of the Defense intelligence agencies conduct name checks with the IGs of those agencies.**
- **Or, direct that the Directors of the Agencies ensure that the Subjects of past Agency IG criminal investigations are titled and indexed in DCII.**

## USD(I) Comments

USD(I) concurred with the recommendation, and will “explore both options by June 30, 2014, and identify the best way forward.”

## Our Response

The USD(I) comment is responsive. We request that USD(I) advise us of its determination by July 15, 2014.

**B. 2.a. We recommend that the Directors of DIA, NGA, NRO, and NSA, in the absence of an overarching DCII policy, evaluate titling and indexing in the DCII the Subjects of all non-criminal investigations conducted by all Agency investigative elements.**

## DIA Comments

DIA concurred with the recommendation, stating that DIA offices currently entered data

into the DCII.

## NGA Comments

NGA concurred with the recommendation. NGA IG obtained full user access to DCII effective August 26, 2013, and will evaluate titling and indexing the Subjects of its non-criminal investigations in DCII. The NGA Office of Security currently had read-only access to DCII, but will request full user access no later than April 30, 2014, so that it can title and index its personnel security investigations and polygraph examinations.

## NRO Comments

NRO non-concurred with the recommendation. NRO stated:

“The NRO has considered this recommendation and interprets ‘non-criminal investigations’ to pertain to personnel security investigations. Individuals determined eligible for and briefed into [SCI] access with a Condition, Deviation, or Waiver are reflected accordingly in Scattered Castles. It is our understanding and interpretation that the [DCII] is no longer used for this purpose, as the report indicates on page 3, second bullet, since personnel security investigative and adjudicative records were removed from the DCII.”

## NSA Comments

NSA non-concurred with the recommendation. NSA stated:

“We disagree with applying Recommendation B(2)(a) to the extent that it would apply to security investigations. The DoD-designed repository for investigations of security significance is [JPAS]. NSA already submits all such cases on DoD contractors to JPAS and to SCATTERED CASTLES (as the IC repository).”

## Our Response

The DIA and NGA comments are responsive to our recommendation.

The NRO and NSA comments are not responsive. Their responses illustrate the confusion – in the absence of an overarching DCII policy -- regarding which investigations by which investigative entities are to be titled and indexed in DCII. It is our understanding that Deputy Secretary Vance intended that all investigations conducted by all DoD investigative entities would be titled and indexed in DCII. Consequently “non-criminal investigations” might reasonably include administrative investigations that the Agency IGs conducted, as well as complaint type personnel security, security violation, unauthorized disclosure, and counterintelligence investigations that the Agency counterintelligence and security elements conducted. Indices on personnel security background investigations and adjudications were moved from DCII to JPAS with the creation of JPAS. Complaint type personnel security

investigations seemingly appear in JPAS only to the extent that information from them is used to populate the incident report fields in JPAS. Because incident report fields in JPAS were not necessarily populated with relevant information from the Agency IG investigations that we examined in this assessment, we are concerned that the same situation is occurring with regard to complaint type personnel security, security violation, unauthorized disclosure, and counterintelligence investigations. Titling and indexing an investigation in DCII provides clear data which may be used by another federal entity to obtain a copy of the investigation from the originator. We request that the Directors, NRO and NSA respectively, reconsider our recommendation to ensure Subjects of investigations are titled and indexed in DCII, and provide additional comments in response to the final report.

**B. 2.b. We recommend that the Directors of DIA, NGA, NRO, and NSA direct their Offices of Security to develop formal procedures to ensure that reports of investigation into misconduct by contractor personnel are reported to DODCAF.**

### DIA Comments

DIA concurred with the recommendation, stating that it already had a process in place in which the DIA Office of Security and DIA IG notified DODCAF of derogatory information regarding contractor personnel.

### NGA Comments

NGA concurred with the recommendation. The NGA Office of Security had adjudicative authority over its contractors and investigated and adjudicated all reports of misconduct by contractor personnel. The Office of Security will enter reports of misconduct by contractor personnel into JPAS and develop formal procedures to ensure that reports of investigation are forwarded to DODCAF no later than June 30, 2014.

### NRO Comments

NRO non-concurred with implementing this recommendation at NRO. NRO stated that:

“A process is already in place that ensures NRO Office of Security and Counterintelligence (OS&CI) reports denials and revocations on contractors with [DoD] equities directly to the [DODCAF]. All other cases involving derogatory information developed on contractors during personnel security processing are reported via Scattered Castles Daily Exception Reports, which are available to DOD. In addition, the NRO OIG reports cases involving misconduct of contractor personnel to OS&CI, and this information is reported via Scattered Castles Daily exception Reports.”

### NSA Comments

NSA concurred with the recommendation, stating that prior to DODCAF's establishment investigations were reported to DISCO. Since then, any cases involving contractor misconduct with a national security clearance eligibility nexus have been reported to

the DODCAF in accordance with internal operating procedures. NSA said it will continue to enforce its internal procedures that require the reporting of any derogatory information regarding DoD contractors to DODCAF.

## Our Response

The DIA, NGA, and NSA responses are responsive to the recommendation. The NRO comments are partially responsive and require no further action.

The NRO response acknowledging that contractor information was being provided to DODCAF highlighted an issue with the DoD personnel security system. Even though JPAS is the Department's personnel security database, NRO uses SCATTERED CASTLES. Paragraph 5.a., DoDD 5105.23, "National Reconnaissance Office," June 28, 2011, designates NRO as a Defense Agency, yet it does not report to, or accept personnel security clearances from, JPAS. This situation further supports Recommendation A.1. regarding the need for an overarching JPAS policy. An overarching policy will either direct NRO to report to JPAS or give it a clear exception to policy.

**B. 2.c. We recommend that the Directors of DIA, NGA, NRO, and NSA ensure that controls are in place to ensure that favorable personnel security adjudicative determinations made with conditions, deviations, or waivers are documented in the "Exception Information" block of the Subject's SCATTERED CASTLES file.**

## DIA Comments

DIA did not respond to the recommendation.

## NGA Comments

NGA concurred with the recommendation, stating that all favorable personnel security determinations made with conditions, deviations, or waivers were being documented in the "Exception Information" block of the Subject's SCATTERED CASTLES file.

## NRO Comments

NRO did not respond to the recommendation.

## NSA Comments

NSA concurred with the recommendation, stating that NSA had provided information to SCATTERED CASTLES since approximately 2002. In accordance with ICD 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to [SCI] and other Controlled Access Program Information," procedures were already in place to ensure that this information was entered into SCATTERED CASTLES.

## Our Response

The NGA and NSA comments are responsive to the recommendation. However, as we stated earlier in this report, we could not determine from the data provided to us whether the CAFs either: a) judged that the substantiated misconduct that the Agency IGs identified was not of sufficient significance to warrant granting clearance/access with conditions, deviations, or waivers; or b) granted clearance/access with conditions, deviations, or waivers, but these exceptions were not documented by the CAFs in the Subjects' SCATTERED CASTLES files. The NGA and NSA responses imply that the misconduct was not regarded as sufficient for clearance/access to be granted with conditions, deviations, or waivers. That operational decision, unless documented as a condition, deviation, or waiver, then becomes binding through the reciprocity process on all other elements of the IC.

Through an inadvertent editing error, we left this recommendation off the Recommendations Table in our coordination draft, which may account for the lack of response from DIA and NRO. We request that the Directors of DIA and NRO respond to the recommendation.

**B.3. We recommend that the Inspectors General of DIA, NGA, NRO, and NSA work with the Offices of Security of those Agencies to ensure that IG reports of investigation into misconduct by contractor personnel are reported to DODCAF.**

## DIA Comments

DIA concurred with the recommendation, stating that DIA already had a process in which DIA IG notified DODCAF.

## NGA Comments

NGA concurred with the recommendation, stating that the NGA IG provided reports of investigation into misconduct by NGA civilians and contractors to the Office of Security for information and re-adjudication. The Office of Security will work with NGA IG to ensure reports of investigation are forwarded to DODCAF, with the process to be in place no later than June 30, 2014.

## NRO Comments

NRO concurred with the recommendation, stating that NRO IG had:

“...a transmittal memorandum template that accompanies all responses sent to the NRO Office of Security and Counterintelligence (OS&CI). This template contains language requesting OS&CI update all appropriate databases upon receipt of a report. The OIG and OS&CI have regularly scheduled meetings to address various issues and the OIG will use this forum to continue working closely with OS&CI and ensure that all OIG investigations are correctly reported.”

## NSA Comments

NSA disagreed with the recommendation as written, stating that:

“As written the proposed Recommendation language could impair the independence of the NSA IG. NSA suggests modifying Recommendation B(3) to clearly state the separate roles for those two organizations, and changing the report to delete the potentially ambiguous ‘work with’ language. Accordingly, we suggest that the Recommendation might state something such as:

“We recommend that the Inspector General of NSA continue to provide IG reports of investigation into substantial misconduct by contractor personnel (or summaries of these reports) to the NSA Office of Security to enable the NSA Office of Security to report to DODCAF, as required.”

“However, effective immediately all NSA OIG reports of contractor misconduct received by the ADS&CI will now be disseminated to DODCAF. The ADS&CI is also implementing a protocol to ensure the OIG is notified when such reports are forwarded.”

## Our Response

The DIA, NGA, and NRO comments are responsive to the recommendation. NSA's interpretation achieves the objective of the recommendation and requires no further action.

**B.4. We recommend that the Director, Defense Human Resources Activity, work with GSA to add EPLS/SAM to the set of databases being accessed by ACES.**

## Defense Human Resources Activity (DHRA) Comments

DHRA non-concurred with the recommendation, stating that it was “premature since analysis of this data is required to include value of data source in identifying issues impacting federal investigative standards, and determining if the use of that data source meets legal, privacy, and Paperwork Reduction Act requirements. Incorporating [EPLS/SAM] into ACES would also require business analysis, software development, interface development, testing and additional funding/resources to accomplish that work.”

## Our Response

DHRA's comments are not responsive to the recommendation. We reiterate that contractors and contractor employees are listed in EPLS/SAM because they have been suspended or debarred for incompetence or misconduct on federal contracts. Misconduct on a federal contract should have a direct bearing on eligibility for personnel security clearance/access. Any future continuous monitoring system should incorporate data from EPLS/SAM. We request that the Director, DHRA, reconsider our recommendation to add EPLS/SAM to the set of databases being accessed by ACES, and

comment in response to the final report. We also request that the Director, DHRA, provide this office with an action plan with milestones to achieve this objective.

## Finding C

---

### Avoidance of Personnel Security Adjudication and Due Process Issues

Agency security offices were avoiding the adjudication of Agency IG investigations after the discovery of employee misconduct and consequently avoiding the initiation of due process.

#### Background

EOs 10865, "Safeguarding Classified Information within Industry," and 12968, "Access to Classified Information," require that personnel, including contractor employees, whose security clearance was denied or revoked be given due process. EO 12968 further requires that personnel security actions shall cease upon termination of the applicant's need for access to classified information. Due process in contractor personnel security cases requires that an employee: a) be advised in writing of the government's intent to revoke or deny security clearance/access; b) be provided access to documentation supporting that conclusion; c) be afforded a reasonable opportunity to respond to the conclusion in writing, including representation by counsel; d) be afforded an opportunity to appear personally before an adjudicative authority; e) be advised in writing of the government's decision; and f) be afforded an opportunity to appeal an unfavorable decision to a high-level panel. DoDD 5220.6 carries out the provisions of EO 12968 by stating: "Actions pursuant to this Directive [that is personnel security actions] shall cease upon termination of the applicant's need for access to classified information except in those cases in which:

- "A hearing has commenced.
- "A clearance decision has been issued; or
- "The applicant's security clearance was suspended and the applicant provided a written request that the case continue."

#### Failure to Implement Due Process Procedures

In many of the IG investigations we reviewed, we found failures to pursue personnel security clearance and due process procedures. As soon as employee misconduct was discovered, the contracting company either fired the employee, or the employee "resigned." Once this occurred, the employee no longer had a need for access to classified information and no further personnel security action was taken. This meant the case was not adjudicated for denial or revocation of security clearance/access, nor was it reported to JPAS except as a "loss of jurisdiction." In JPAS it appeared that the contractor employee was still eligible for a security clearance.

DIA Office of Security (SEC) staff described a process they used, which was a creative variation on this theme. Due to limited resources to conduct formal adjudications which would result in due process actions, when SEC received a DIA IG investigation appearing to warrant adverse action regarding contractor employees' security clearance/access, SEC terminated their *physical* access to DIA facilities by confiscating



security badges and having DIA police escort them from the facility. Because most contractor employees were hired to work on a specific project at a specific location, terminating physical access generally led the contracting company to fire its employee.

SEC then posted an entry (“Z” Code) in JPAS, reporting a “loss of security jurisdiction.” In the future, knowledgeable security professionals would understand that if they saw a “Z” code regarding a potential contractor employee, they should contact SEC to receive further information on that individual. No *formal* adjudicative determination by the DIA CAF existed regarding the contractor employee’s clearance/access to classified material. Additionally, after three years, the contractor employee’s paper file was destroyed.

Therefore, during a future background investigation, OPM potentially would never discover the IG report of investigation unless the OPM background investigation scope sheet contained a requirement that the investigator consult with the Agency IG. OPM staff told us that OPM investigators only conducted file checks with the Agency IGs when an IG investigation was titled and indexed in DCII, or when the investigation developed a lead indicating that the IG might have an investigative record.

Another technique that Offices of Security used was “withdrawing of eligibility for security clearance/access.” Because a security clearance was not denied or revoked, no requirement existed for due process, even though the functional result -- i.e., the Subject no longer had access to classified material and could no longer hold a job requiring such access -- was the same. Under these circumstances, a possibility existed of one of two events occurring:

- Contractor employees would go into a “security limbo” in which they would not receive due process; their misconduct would not be adjudicated; their security clearance would not be revoked or denied; and they would not be granted access to classified information or facilities.
- Or, contractor employees would be granted security clearances/access in another location at a later time.

## Conclusions

The requirements of EOs 10865 and 12968 for due process in the revocation or denial of contractor employees’ security clearances/access have led to an avoidance of personnel security adjudications. On the part of government agencies, this results from an effort to avoid time and resource intensive due process procedures. On the part of contracting companies, it may result from an understanding that a preemptive “termination” or “resignation” could reduce the potential for suspension or debarment, and might also preserve the contractor employee’s security clearance/access eligibility for possible future use.

## Recommendation, Management Comment, and Our Response

**C. We recommend that USD(I) initiate the process to revise EO 12968 by requiring that in substantiated misconduct cases personnel security clearance adjudicative actions continue, even if the contractor employee has been terminated and/or no**

**longer has access to classified information. If the misconduct is sufficient to warrant denial or revocation of security clearance/access, then that action should be formally accomplished.**

### USD(I) Comments

USD(I) concurred with the recommendation, and offered to submit our recommendation to the Director of National Intelligence, who is responsible for coordinating national personnel security policy with the Executive Office of the President.

### Additional DIA Comments

Although DIA was not required to comment, it disagreed with the recommendation, stating that:

“Recommending that actions continue in the case of a contractor that no longer requires an eligibility determination to be rendered is counter to and inconsistent with being good stewards of the taxpayer money and the Office of the Director of National Intelligence policy that only those that require access are granted eligibility. An appropriate notation entered into [JPAS] and Scattered Castles would be sufficient to provide information to a future adjudicative authority.”

### Our Response

USD(I)'s proposed course of action is responsive to the recommendation. With regard to DIA's comment, we note that of the 94 IG investigative Subjects listed in JPAS, only 35 percent of the Subjects had relevant information contained in the incident report blocks of their JPAS files.

## Finding D

---

### Lack of Personnel Security Information Sharing

IC and DoD personnel security policies broadly require the reporting of unfavorable personnel security information. We noted a lack of external information sharing regarding security clearance investigations and adjudications. This condition occurred because of the lack of policy, recordkeeping, and proper security adjudication/due process. As a result, contractor employees with previous, adverse/questionable, and closed intelligence agency IG investigations were being inappropriately granted security clearance/access with other IC elements.

### Internal Personnel Security Information Sharing

If a particular Agency IG conducted an investigation and presumably completed a report of investigation, it seemed reasonable to assume that the CAF of that same Agency would in the future have been able to access that report of investigation and make a fully informed adjudicative judgment. From the Agency IG investigations we reviewed, we noted only three instances where this situation did *not* occur.

In two NSA cases, the NSA IG told us it had sent a copy of its reports of investigation to the NSA Office of Security; however, the NSA Office of Security said it did *not* receive the reports and had consequently taken no adjudicative action. In one DIA case, DIA CAF told us that the security files of the two Subjects did *not* contain the DIA IG report of investigation and that no security action was taken regarding those Subjects.

### Lack of External Personnel Security Information Sharing

We found that contractor employees were retaining security clearance/access – or were being granted security clearances/access by another CAF at a later time. Of the cases we reviewed, 45 percent (57 out of 128) of the Subjects continued to hold or were re-granted security clearance/access *after* Agency IG investigations were closed.

After reviewing this data, we conducted data calls to several CAFs to see if any of the CAFs had made a favorable security/access adjudicative determination on a Subject who had been investigated by another Agency's IG. We sought to determine if information had flowed from one agency to another, which would give that agency the ability to make a fully-informed adjudicative determination.

We noted one case in which an external agency CAF was aware of a Defense intelligence agency IG investigation at the time that CAF adjudicated the Subject for security clearance/access. In 2006, one Subject was debriefed by the NRO Office of Security, and was titled and indexed in DCII by DCIS in 2007. SCATTERED CASTLES indicated that the Subject was then briefed for a "Q" clearance by the Department of Energy (DoE) from 2011-2012. DoE told us it *was* aware of the NRO IG report of investigation at the time it made its favorable adjudicative decision.

In all the remaining cases covered by our data calls, the CAFs of other IC elements were unaware of the earlier Defense intelligence agency IG investigations. Summaries of some of these cases follow:

DCIS and DIA IG had investigated a Subject. Later, the Department of Homeland Security (DHS) -- unaware of the earlier DCIS/DIA IG investigation -- granted the Subject SCI access under reciprocity, based on DIA's adjudication. Then, in 2012, DHS debriefed the Subject from SCI.

SCATTERED CASTLES indicated the Subjects of two NRO IG investigations were later briefed for SCI by DIA. DIA CAF told us that:

- It had no adjudicative record of the Subject of one NRO IG case.
- It could not locate its paper adjudicative file on the Subject of the second NRO IG case, and its electronic index did not indicate whether the case was adjudicated with knowledge of the NRO IG investigation.

Eight Subjects of three NSA IG cases, four NRO IG cases, and one DIA IG case, were later briefed for SCI by the Central Intelligence Agency (CIA). Regarding those Subjects, the CIA told us that:

"CIA Clearance Division reviewed the security records of the eight individuals highlighted in the DOD IG request. All eight individuals were originally briefed (crossed over) by CIA based on adjudicative guidelines for reciprocity of another agency's positive adjudicative decision. Depending on when the approval was made (processing varied based on the tools available at the time of the review) CIA reviewed JPAS, DCII, and/or Scattered Castles prior to making a determination, based on standard guidelines. On four of the eight individuals, our records indicate that CIA received adverse information subsequent to the crossover decision. As a result two were denied access, one is undergoing a reinvestigation, and the other requires an event driven action. CIA was unaware of the IG investigations of the other four individuals until the DOD IG request. Of those four, three remain in access at this time. As a result of the supplied information, CIA will be reviewing their records and initiating personnel security processing as appropriate."

As stated earlier in this report, we provided our list of 128 investigative Subjects to DODCAF and asked it to review its files to determine if its predecessor CAFs had received copies of the related investigative reports that the Agency IGs prepared. DODCAF answered that it could only positively determine whether or not it had received an Agency IG report on 20 percent of the Subjects (26 of 128); for those Subjects, it had only received five reports -- all of them on NRO IG investigative Subjects.

## Results of Lack of Personnel Security Information Sharing

The misconduct documented in the IG investigations we reviewed did not result in suspension or debarment, or generally in prosecution; furthermore, for 45 percent of the Subjects (57 of 128) it did not result in permanent denial or revocation of security

clearance/access to classified material.

- OPM has not routinely cross-checked the names of Defense intelligence agencies' current/former employees, military assignees, and contractor employees with the IGs of those agencies.
- Withdrawing either a) physical access to facilities; or b) eligibility for access to classified materials in lieu of formal denial or revocation of security clearance/SCI access appears to be a deliberate effort to avoid personnel security adjudication and the due process requirements for contractor employees contained in EOs 10865 and 12968, and DoDD 5220.6.

<b>Personnel Who Held Security Clearance/Access Following Closure of an IG Investigation*</b>			
<b>IG Office Conducting Investigation</b>	<b>Number of Cases**</b>	<b>Number of Individual Subjects</b>	<b>Number of Subjects Who Held Clearance/Access Following Closure of an IG Investigation***</b>
DIA	20	21	15
NGA	3	3	0
NRO	80	76	25
NSA	28	28	17
<b>TOTAL</b>	<b>131</b>	<b>128</b>	<b>57</b>

\* Based on Data from JPAS and SCATTERED CASTLES.

\*\* Of the 131 cases, two were duplicate reports and 12 involved exclusively corporate Subjects with no individual Subjects identified.

\*\*\* Some of the Subjects held or retained clearance/access that multiple agencies granted following the conclusion of the IG investigation in which they were titled.

## Conclusion

We found throughout this assessment that the appropriate DoD and IC databases were not being populated with information on the Subjects of substantiated Defense intelligence agency IG investigations. This affected the ability of CAFs across the IC to conduct fully informed personnel security clearance/access adjudications. The population of investigative and personnel security databases with accurate and complete information is absolutely critical in preventing unsuitable individuals from obtaining sequential personnel security clearance/access.

## Recommendation D

We believe that our earlier recommendations (i.e., Recommendations A, B, and C) will enable effective internal and external information sharing.

## Finding E

---

### Lack of Connectivity Between DCII and JPAS

No vehicle exists for entries in DCII to automatically flag JPAS. As a result, if a personnel security adjudicator with authorized access queries JPAS regarding a specific Subject, no mechanism exists in JPAS to tell the adjudicator that DCII also contains an entry.

### Background

In June 2010, the Deputy Secretary of Defense directed that operational responsibility for JPAS and DCII be transferred from DSS to DMDC.

There was *extremely* limited connectivity between JPAS and DCII. DMDC staff told us no vehicle currently existed for entries in DCII to automatically flag JPAS. Therefore, if a personnel security adjudicator with authorized access queried JPAS regarding a specific Subject, no mechanism existed in JPAS to tell the adjudicator that DCII also contained an entry. To determine if a Subject had a DCII entry, the adjudicator would have to use a second password and authenticator to transfer from JPAS to DCII.

Thus, although DCII's purpose is to ensure that investigative information on Subjects titled and indexed in DCII can be retrieved at a later time, DCII does not have an interface with JPAS to alert security adjudicative personnel.

### Conclusion

The current lack of connectivity between DCII and JPASS does not facilitate the identification of investigative information titled and indexed in DCII by authorized personnel security adjudicative staff.

### Recommendation, Management Comments, and Our Response

**E. We recommend that the Director, Defense Human Resources Activity, develop software to automatically flag the Case Adjudication Tracking System (CATS) of the Defense Information System for Security (DISS) family of systems that a DCII file exists on a specific Subject.**

### Defense Human Resources Activity (DHRA) Comments

In our coordination draft we recommended that DHRA develop software to automatically flag the personnel security adjudicative portion of JPAS that a DCII file existed on a specific Subject. DHRA concurred with that recommendation, but provided the following clarification: that software should be developed to "automatically flag the personnel security adjudicative portion of the Case Adjudication Tracking System (CATS) that a [DCII] file exists on a specific subject. CATS, and not [JPAS], is now the primary personnel security system that the [DODCAF] uses for adjudication purposes.

CATS is one component of the Defense Information System for Security (DISS) family of systems.”

### Our Response

DHRA’s comments are responsive. Because JPAS is becoming a legacy system as the Department moves toward DISS, we concur with DHRA’s exception to our draft recommendation and accordingly changed the recommendation.

## Other Observation

---

### Observation A

#### ***Similar Issues with DoD Civilian and Military Personnel***

This study was conducted specifically with regard to a sample of unclassified investigative summaries involving *contractor* employees. We note that the case summaries contained in the *Classified Annexes to the [DoD IG's] Semi-Annual Report to Congress* involving contractor employees were significantly outnumbered by those on civilian and military Subjects assigned to the Defense intelligence agencies. We believe further evaluation is needed regarding security clearance/access processing for the Defense intelligence agencies' *civilian* employees and *military* personnel. We will review this matter and work with the Agency IGs to determine appropriate scope and at what level the review should take place.



# Appendix A

## Background

On September 5, 2012, this office published the memorandum report, *The Four Defense Intelligence Agencies Have Had No Effective Procedures for Suspension and Debarment*. That report's objective was to determine if the four Defense intelligence agencies -- DIA, NGA, NRO, and NSA -- had carried out basic and effective suspension and debarment procedures. We found that none of the Agencies had ever debarred a contractor, consultant, or contractor employee. We also found that only one of the Agencies -- NSA -- had ever suspended a contractor, consultant, or contractor employee: NSA suspended three individuals in 2011 following their felony convictions in federal court.

During our research for that project, we found that procurement and counsel staff assumed that Subject contractor employees involved in misconduct would lose their security clearance and access. We examined this theory using the same 131 cases that we had used in the suspension and debarment study. Furthermore, the contention ignored the fact that -- absent suspension or debarment -- individuals involved in misconduct that the Agency IGs investigated could work on unclassified government contracts even if they had lost their security clearance and SCI access.

Prior to October 1, 2010, DoD IG published the *Classified Annex to the [DoD IG's] Semi-Annual Report to Congress*. The *Annex* was largely a compendium of significant audit and investigative case summaries that the Agency IGs provided. With their increased statutory authorities as IGs of Designated Federal Entities under the Inspector General Act of 1978, as amended, the IGs began publishing their own semi-annual reports to Congress, circa April 2011. As part of our research for the suspension and debarment study, we reviewed *Annexes* covering the period from October 1, 2000, through September 30, 2010. The case summaries indicated that the IGs had achieved some success in identifying and investigating misconduct by individual contractor employees, and that their efforts had generally improved over time. From *Annexes* covering that 10-year period, we selected 131 unclassified investigative case summaries involving contractors in the Defense intelligence community. Our selection of cases represented a judgmental sample at several levels. First, in determining which cases to report to us, the IGs had made their own judgments regarding which cases were "significant." Secondly, we selected only unclassified case summaries from the *Annexes* in a deliberate effort to make *The Four Defense Intelligence Agencies Have Had No Effective Procedures for Suspension and Debarment* available for the widest possible dissemination.

Sixty-eight percent of these cases (89 out of 131) involved time-and-attendance fraud by individual contractor employees or groups of contractor employees. In the 86 cases involving individual employees, the loss per employee ranged from \$433.00 to \$265,698.00. The median loss was \$32,443.88, and the average loss was \$41,788.96. In the 89 time-and-attendance cases, the aggregate loss was \$4,336,140.40. In most instances, these losses were fully recouped from the contractors' employers. Therefore, a widespread belief existed among the personnel security staff and at the Department of Justice that recouping the losses made the government "whole" again, thereby reducing the need for further action.

We expected virtually all of the Subjects to be referred to the appropriate CAF for security clearance/SCI access adjudication. However, our current review proved that this did not necessarily occur. The DoD personnel security program's purpose is to ensure that granting federal employees, military personnel, contractor employees, and other affiliated persons access to classified information is clearly consistent with U.S. national security. In considering the continuum of misconduct documented in the IG investigations, a point is reached when the ability of the contract employee to responsibly hold a security clearance and have SCI access must be questioned.

## Appendix B

---

### Scope and Methodology

This evaluation was conducted from September 2012 to January 2014, in accordance with Quality Standards for Inspection and Evaluation that the Council of the Inspectors General on Integrity and Efficiency issued. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. To accomplish our objectives we:

- Reviewed applicable EOs, and DNI and DoD personnel security policy.
- Sent data calls to the four Defense intelligence agency IGs asking them to provide biographic information -- name, employer, employer Commercial And Government Entity (CAGE) code, date and place of birth, and social security number -- for the individuals they had identified as Subjects of their 131 investigations. We also asked for the security clearance and access level of these Subjects at the time of the IG investigations, and whether the IG had referred a copy of their report of investigation to their Agency CAF or any other CAF. In response to this data call, the Agency IGs identified 128 individual Subjects. All subsequent data calls depended upon the accuracy of the responses to this data call.
- Received the data provided by the Agency IGs and sent data calls to the DIA, NGA, NRO, and NSA CAFs, and to DODCAF requesting that they determine if they had received copies of the IG reports of investigation, if they had conducted security clearance/access adjudications as a result of the reports, and the results of those adjudications.
- Discovered that some contractor employees held security clearance and access with subsequent agencies following the closure of the first agency's IG investigation, therefore we sent limited additional data calls to determine if the subsequent agency's CAF was aware of the first agency's IG investigation.
- Interviewed personnel from DIA, NGA, NRO, NSA, DODCAF, DMDC, and OPM regarding procedures at their organizations, and requested they provide supporting agency documentation.
- Conducted checks in DCII and SCATTERED CASTLES on the Subjects identified by the Agencies' IGs. The SCATTERED CASTLES database is the IC's authoritative personnel security repository for verifying personnel security access approvals regarding SCI and other controlled access programs. By using SCATTERED CASTLES rather than JPAS, we were able to determine if the

individual Subjects of the IG investigations had subsequently held security clearance/access not only with DoD entities, but within the IC outside of DoD.

- Noted some anomalies in our data, and ultimately requested that DMDC provide information from the Subjects' files in JPAS.
- Culled data from a variety of sources and databases. During our effort, we noted data anomalies which we were unable to fully resolve. This report represents our best effort to coherently integrate the information provided to us.

## Limitations

We did not evaluate the personnel security adjudicative decisions that the CAFs made. It is within the scope of authority of the Directors of the Defense intelligence agencies and DODCAF to grant security clearance/access within adjudicative guidelines to those they believe appropriate in achieving the Agencies' and DoD's operational missions. We also note that operational needs, the passage of time, and other mitigating factors may override adverse personnel security adjudicative decisions.

# Appendix C

## Office of the Under Secretary of Defense for Intelligence Response to Our Draft Report



INTELLIGENCE

OFFICE OF THE UNDER SECRETARY OF DEFENSE  
5000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-5000

FEB 19 2014

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Response to DoD IG Draft Report, "An Assessment of Contractor Personnel Security Clearance Processes in the Four Defense Intelligence Agencies (Project No. D2013-DINT01-0009.000), January 28, 2014

In response to the January 28, 2014 request for comments on an update to OIG Report D-2006-077, we provide the following responses pertaining to DoD IG recommendations for the Office of the Under Secretary of Defense for Intelligence (USD(I)).

- **Recommendation A.1:** Develop and issue an overarching policy governing Joint Personnel Adjudication System (JPAS) operation.

**USD(I) Response:** USD(I) concurs with this recommendation. Given the challenges inherent to the government policy issuance process, we have issued JPAS policy via memoranda over the past several years and agree that a consolidated overarching policy is needed. DoDM 5200.02 Volume 1, "DoD Personnel Security Program (PSP): Investigations for National Security Positions and Duties" and DoDM 5200.02 Volume 2, "DoD Personnel Security Program (PSP): Adjudications, Due Process, Continuous Evaluation and Security Education, as described below, each provide overarching policy governing operation of JPAS and its successor system (the Joint Verification System), to include requirements for recording issues of security concern and adjudications that are based on exceptions due to presence of adverse information. Since Volume 2 is still in the formal comment period, we have an immediate opportunity to ensure that we incorporate the IG's recommendations and address the need for JPAS functionality as discussed in the IG report.

- **Recommendation A.2:** Coordinate with Office of Management and Budget (OMB) to finalize updates to – or replacements for – the following Departmental policies:

**USD(I) Response:** USD(I) concurs with the recommendation to finalize updates or replacements for the policies. We do suggest nuancing the recommendation to reflect the diversity of roles and responsibilities that pertain to the policies that are of concern to the DoD IG. To assist in appropriate revisions, we provide more detail about the ownership and status of the policies listed in Recommendation A.

- a. DoD Directive (DoDD) 5220.6, "Defense Industrial Personnel Security Clearance Review Program," April 4, 1999

**Status:** DoDD 5220.6 does not fall under the authorities of the USD(I). It is issued by the DoD General Counsel (DoD GC). The DoD IG should correct the findings to assign responsibility for this recommendation to the DoD GC.

- b. DoD 5200.2-R, "Personnel Security Program," February 23, 1996



**Status:** The DoD 5200.2-R is being replaced by DoDM 5200.02 Volume 1, "DoD Personnel Security Program (PSP): Investigations for National Security Positions and Duties" and DoDM 5200.02 Volume 2, "DoD Personnel Security Program (PSP): Adjudications, Due Process, Continuous Evaluation and Security Education."

Volume 1 has been in the Office of the General Counsel, Intelligence (OGC(I)) since July 29, 2013 for legal sufficiency review. Following the OGC(I) review, OUSD(I) will expedite making any required changes before moving the policy to DoD OGC for approval. Thereafter, USD(I) is required to coordinate with the Washington Headquarters Service (WHS) Federal Register Liaison Office (FRLO) which coordinates with OMB to meet OMB's requirements for publishing the policy as a federal rule.

The formal coordination of Volume 2 closed January 17, 2014. USD(I)'s goal is to complete adjudication of comments by March 7, 2014. Thereafter, the policy issuance process will proceed according to steps established by WHS as published at [http://www.dtic.mil/whs/directives/corres/writing/DOD\\_process\\_home.html](http://www.dtic.mil/whs/directives/corres/writing/DOD_process_home.html) and according to timelines established by the Director of Administration and Management in DoD Instruction 5025.01, "DoD Directives Program." Once through the DoD policy issuance process, USD(I) is again required to coordinate with the WHS FRLO to navigate the proposed policy through OMB's rule making process.

- c. DoD 5220.22-R, "Industrial Security Regulation," December 1985.

**Status:** The DoD 5220.22-R will be replaced by DoD 5220.22M Volume 2, "National Industrial Security Program: Industrial Security Procedures for Government Activities." The DoD will work with WHS who coordinates with OMB to publish the policy through OMB's Federal Register process. The DoD is currently working with OMB to format the volume and to complete information collections according to OMB requirements (e.g., approval of a revised DD Form 254, "Contract Security Classification Specification").

- d. DoD 5220.22-M, "National Industrial Security Program: Operating Manual," February 28, 2006

**Status:** The DoD 5220.22-M was updated and posted to the Washington Headquarters Service Website for DoD Issuances on March 28, 2013.

- e. DoD 5220.22-M-Sup 1, "National Industrial Security Program: Operating Manual Supplement," February 1995.

**Status:** DoD 5220.22-M-Sup 1 will be canceled when the next conforming change to DoD 5220.22-M is approved. The policy is currently being processed through the formal DoD policy issuance process. Our goal is to issue the conforming change by January 1, 2015.

- **Recommendation B.1.a:** Prepare an overarching policy governing the operation of DCII, including identification of the categories of investigations to be title and indexed, and the retention criteria for investigations so titled and indexed.

**USD(I) response:** Concur. We will convene a working group to develop, as appropriate, overarching policy governing the operation of the DCII by September 30, 2014.

- **Recommendation B.1.b:** Direct the Defense Intelligence Agencies to review the procedures that their Offices of Security use to ensure that JPAS and Scattered Castles are being properly populated.

**USD(I) response:** Concur. USD(I) will issue a memorandum directing the recommended review by April 15, 2014.

- **Recommendation B.1.c:** Direct the Defense Intelligence Agencies to ensure that the Subjects of Agency IG criminal investigations are titled and indexed in DCII in accordance with DoDI 5505.16.

**USD(I) response:** We concur with the recommendation to ensure that the subjects of IG criminal investigations are titled and indexed in the DCII. We will work with the DoD IG to determine the correct authorities for issuing such a requirement.

- **Recommendation B.1.d:** Ensure that subjects of past investigations are titled and indexed in the DCII either by requiring OPM to conduct checks of Defense Intelligence Agencies' IG records or directing the Directors of the DoD Intelligence Agencies to ensure that subjects of past IG criminal investigations are titled and indexed in the DCII.

**USD(I) response:** We concur with the recommendation to ensure that past investigations are accessible in background investigations for determining eligibility for access to classified information. USD(I) will explore both options by June 30, 2014 and identify the best way forward.

- **Recommendation C:** Initiate the process to revise EO 12968 by requiring that in substantiated misconduct cases, personnel security clearance adjudicative actions continue, even if the contractor employee has been terminated and/or no longer has access to classified information.

**USD(I) response:** Concur. To initiate the process, we will submit the IG's recommendation to the Security Executive Agent (i.e., the Director of National Intelligence pursuant to EO 13467) who, in turn, is responsible for coordination of national personnel security policy with the Office of Management and Budget's Executive Office of the President.

We appreciate the opportunity to respond to your draft report. My point of contact is [REDACTED].

  
HM Higgins  
Director for Defense Intelligence  
(Intelligence & Security)

# Appendix D

## Defense Intelligence Agency Response to Our Draft Report



### DEFENSE INTELLIGENCE AGENCY

U-14-85,023/SEC

February 18, 2014

#### **Defense Intelligence Agency Comments on the Draft Report for Review: An Assessment of Contractor Personnel Security Clearance Processes in the Four Defense Intelligence Agencies**

*This paper responds to a request to review and comment on the above referenced draft report from the Department of Defense (DoD) Inspector General (IG).*

Findings and recommendations provided by the DoD IG illustrate the inconsistency of the information provided and available to the adjudicative offices in the Intelligence Community. When information regarding a contractor is missing from any one or all of the available databases, it is possible for subjects to move from one contract vendor to another or from one agency to another without completing the security processing in the previous assignment.

#### **Response to Recommendations Specific to Defense Intelligence Agency (DIA)**

- Recommendation B.2.a. DIA agrees with this recommendation. DIA offices currently enter data into the Defense Central Index of Investigations.
- Recommendation B.2.b. DIA agrees with this recommendation. DIA already has a process in place by which the DIA Office of Security and DIA IG notifies the Department of Defense Consolidate Adjudication Facility (DoDCAF) of derogatory information regarding contractor personnel.
- Recommendation B.3. DIA agrees with this recommendation. DIA already has a process by which DIA IG notifies the DoDCAF.

#### **(U) Responses to Recommendations Other Than DIA Specific Recommendations**

- Recommendation C. DIA disagrees with this recommendation. Recommending that actions continue in the case of a contractor that no longer requires an eligibility determination to be rendered is counter to and inconsistent with being good stewards of the taxpayer money and the Office of the Director of National Intelligence policy that only those that require access are granted eligibility. An appropriate notation entered into Joint Personnel Adjudication System and Scattered Castles would be sufficient to provide information to a future adjudicative authority.

cc: Defense Intelligence Agency, Director  
Defense Intelligence Agency, Inspector General  
Defense Intelligence Agency, Office of Security

*One Mission. One Team. One Agency.*  
Committed to Excellence in Defense of the Nation



Prepared by: [REDACTED], Directorate for Mission Services, Office of Security, Personnel  
Security Division, Staff Director, [REDACTED].



Stephen R. Norton  
Director of Security

# Appendix E

## National Geospatial-Intelligence Agency Response to Our Draft Report



UNCLASSIFIED//  
NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY  
7500 GEORGE MEADE DRIVE  
SPRINGFIELD, VIRGINIA 22150

FEB 19 2014

U-2014-0326

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE  
DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE AND  
SPECIAL PROGRAM ASSESSMENTS, DEPARTMENT OF  
DEFENSE

SUBJECT: (U) National Geospatial-Intelligence Agency Response to Project  
No. D2013-DINT01-0009.000

REFERENCE: (U) "An Assessment of Contractor Personnel Security Clearance  
Processes in the Four Defense Intelligence Agencies" (Project  
No. D2013-DINT01-0009.000), 28 January 2014

1. (U) Thank you for the opportunity to comment on the subject draft report. This memo is in response to the recommendations issued in the reference.

2. (U) Recommendation B.2.a.

a. (U) Department of Defense Inspector General (DoDIG) Recommendation: "That the Directors of the DIA, NGA, NRO, and NSA in the absence of an overarching DCII policy, evaluate titling and indexing in the DCII the Subjects of all non-criminal investigations conducted by all Agency investigative elements."

b. (U) National Geospatial-Intelligence Agency (NGA) Response: NGA concurs with the recommendation. The NGA Office of Security (SIS) will evaluate titling and indexing in the Defense Central Index of Investigations (DCII) database. SIS currently has only view access to the DCII. Authority for DCII full user access would allow NGA to index personnel security investigations and polygraph examinations, in addition to Inspector General (IG) investigations. SIS will request DCII full user access no later than 30 April 2014. As of 26 August 2013, the NGA Office of Inspector General (OIG) has its own DCII account with full access to DCII, including the ability to perform titling and indexing. NGA OIG will evaluate titling and indexing of subjects of OIG non-criminal investigations in DCII.

3. (U) Recommendation B.2.b.

a. (U) DoDIG Recommendation: "That the Directors of DIA, NGA, NRO, and NSA direct their Offices of Security to develop formal procedures to ensure that reports of investigation into misconduct by contractor personnel are reported to DoDCAF."

b. (U) NGA Response: NGA concurs with the recommendation. SIS has adjudicative authority over DoD contractors and investigates and adjudicates all reports of misconduct on contractor personnel. SIS will enter reports of misconduct by contractor

UNCLASSIFIED//

UNCLASSIFIED// [REDACTED]

SUBJECT: (U) National Geospatial-Intelligence Agency Response to Project No. D2013-DINT01-0009.000

personnel into the DoD Joint Personnel Adjudication System and will develop formal procedures to ensure that reports of investigation are forwarded to the DoD Consolidated Adjudication Facility (CAF) no later than 30 June 2014.

4. (U) Recommendation B.2.c.

a. (U) DoDIG Recommendation: "That the Directors of DIA, NGA, NRO, and NSA ensure that controls are in place to ensure that favorable personnel security adjudicative determinations made with conditions, deviations, or waivers are documented in the 'Exception Information' block of the Subject's SCATTERED CASTLES file."

b. (U) NGA Response: NGA concurs with the recommendation. All favorable personnel security determinations made with conditions, deviations, or waivers are documented in the "Exception Information" block of the subject's SCATTERED CASTLES file.

5. (U) Recommendation B.3.

a. (U) DoDIG Recommendation: "That the Inspectors General of DIA, NGA, NRO, and NSA work with the Offices of Security of those Agencies to ensure that IG reports of investigation into misconduct by contractor personnel are reported to DoDCAF."

b. (U) NGA Response: NGA concurs with the recommendation. The NGA OIG provides reports of investigations into misconduct by NGA civilian and contractor employees to the SIS for information and re-adjudication purposes. SIS will continue to work with OIG to ensure reports of investigation are forwarded to the DoDCAF. This process will be in place no later than 30 June 2014.

6. (U// [REDACTED]) The NGA points of contact for this matter are [REDACTED], External Liaison, Office of Inspector General, who can be reached at [REDACTED] or [REDACTED], and [REDACTED], Division Chief, Security and Installations Directorate, Personnel Security Division, who can be reached at [REDACTED] or [REDACTED].

  
Letitia A. Long  
Director

cc: Under Secretary of Defense for Intelligence

2  
UNCLASSIFIED// [REDACTED]

# Appendix F

## National Reconnaissance Agency Response to Our Draft Report



Office of the Director

UNCLASSIFIED

NATIONAL RECONNAISSANCE OFFICE  
14675 Lee Road  
Chantilly, VA 20151-1715

21 February 2014

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: National Reconnaissance Office Response to Department of Defense, Inspector General Draft Report

REFERENCE: Inspector General, Department of Defense Memorandum and Draft Report, An Assessment of Contractor Personnel Security Clearance Processes in the Four Defense Intelligence Agencies (Project No. D2013-DINT01-0009.000), 28 Jan 14

Thank you for your work on the above referenced subject and the opportunity to comment on the recommendations identified for the National Reconnaissance Office (NRO). The draft report recommendations table on page iv indicates that responses are required from the Director, NRO for Recommendations B.2.a and B.2.b, and the Office of Inspector General (OIG) for Recommendation B.3.

The NRO's consolidated response and comments on the Recommendations are as follows:

a. Recommendation B.2.a. In the absence of an overarching DCII policy, evaluate titling and indexing in the DCII the Subjects of all non-criminal investigations conducted by all Agency investigative elements.

The NRO disagrees with implementing Recommendation B.2.a at the NRO. The NRO has considered this recommendation and interprets "non-criminal investigations" to pertain to personnel security investigations. Individuals determined eligible for and briefed into Sensitive Compartmented Information (SCI) access with a Condition, Deviation, or Waiver are reflected accordingly in Scattered Castles. It is our understanding and interpretation that the Defense Central Index of Investigations (DCII) is no longer used for this purpose, as the report indicates on page 3, second bullet, since personnel security investigative and adjudicative records were removed from the DCII.

b. Recommendation B.2.b. Direct their Offices of Security to develop formal procedures to ensure that reports of investigation into misconduct by contractor personnel are reported to the DODCAF.

UNCLASSIFIED

UNCLASSIFIED

SUBJECT: National Reconnaissance Office Response to Department of Defense, Inspector General Draft Report

The NRO disagrees with implementing Recommendation B.2.b at the NRO. A process is already in place that ensures NRO Office of Security and Counterintelligence (OS&CI) reports denials and revocations on contractors with Department of Defense (DOD) equities directly to the Department of Defense Central Adjudication Facility (DODCAF). All other cases involving derogatory information developed on contractors during personnel security processing are reported via Scattered Castles Daily Exception Reports, which are available to DOD. In addition, the NRO OIG reports cases involving misconduct of contractor personnel to OS&CI, and this information is reported via Scattered Castles Daily Exception Reports.

c. Recommendation B.3. We recommend that the Inspectors General of DIA, NGA, NRO and NSA work with the Offices of Security of those Agencies to ensure that the IG reports of investigation into misconduct by contractor personnel are reported to DODCAF.

The NRO Inspector General agrees with including Recommendation B.3 for the NRO. The NRO OIG has a transmittal memorandum template that accompanies all responses sent to the NRO OS&CI. This template contains language requesting OS&CI update all appropriate databases upon receipt of a report. The OIG and OS&CI have regularly scheduled meetings to address various issues and the OIG will use this forum to continue working closely with OS&CI and ensure that all OIG investigations are correctly reported.

Questions concerning this response may be directed to my OS&CI point of contact, [REDACTED], Personnel Security Division, at [REDACTED].

  
Betty J. Sapp

Attachment:  
(U) SD Form 818, Jul 10

2

UNCLASSIFIED

UNCLASSIFIED

COMMENTS MATRIX FOR DoD ISSUANCES: Contractor Personnel Security Clearance Evaluation							
<i>(Please read instructions on back before completing form.)</i>							
#	CLASS	COMPONENT AND POC NAME, PHONE, AND E-MAIL	PAGE #	PARA #	COMMENT TYPE (C/S)	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	A/R/P
1	U	NRO/OIG [REDACTED]	9	1	S	<p><b>Coordinator Comment:</b> The Office of Inspector General (OIG) has a point of clarification in the report. The OIG believes that one of our investigators may have misspoken when interviewed. The OIG has never had access to the Defense Criminal Index of Investigations (DCII) database. The OIG has always relied on the NRO Office of Security and Counterintelligence to title and index subjects of OIG investigations in the appropriate system(s) of record.</p> <p><b>Coordinator Justification:</b></p> <p><b>Originator Justification for Resolution:</b></p>	
						<p><b>Coordinator Comment:</b></p> <p><b>Coordinator Justification:</b></p> <p><b>Originator Justification for Resolution:</b></p>	
						<p><b>Coordinator Comment:</b></p> <p><b>Coordinator Justification:</b></p> <p><b>Originator Justification for Resolution:</b></p>	
						<p><b>Coordinator Comment:</b></p> <p><b>Coordinator Justification:</b></p> <p><b>Originator Justification for Resolution:</b></p>	

# Appendix G

## National Security Agency Response to Our Draft Report



UNCLASSIFIED

NATIONAL SECURITY AGENCY  
FORT GEORGE G. MEADE, MARYLAND 20755-0000

25 February 2014

MEMORANDUM FOR DEPUTY ASSISTANT INSPECTOR GENERAL FOR  
INTELLIGENCE EVALUATIONS

SUBJECT: An Assessment of Contractor Personnel Security Clearance Process in the Four  
Defense Intelligence Agencies (Project No. D2013-DINT01-0009.000) – ACTION  
MEMORANDUM

(U) Per your 28 January 2014 request for comments from the Director of NSA concerning the Recommendations set forth in your draft Assessment of Contractor Personnel Security Clearance Processes in the four Defense Intelligence agencies (hereafter, Report), we address two general points, as well as the specific subsections within Finding B, Lack of Effective Recordkeeping, as they apply to NSA.

(U) The first general point concerns page five, Finding B, Lack of Effective Recordkeeping. The basis upon which you find that the NSA Office of the Inspector General (OIG) lacked effective recordkeeping is unclear. The OIG provided all of the DoD IG-requested documents, and to our knowledge, the OIG was neither interviewed nor otherwise requested to provide information regarding recordkeeping practices. To the extent that the finding stems from evidence that the investigative and personnel databases, particularly the Defense Central Index of Investigation (DCII), were not reliably populated, the OIG believes that this problem may stem from a lack of overarching policy governing DCII operations.

(U) The second general point is that the statement on page 11 of the Report that “[d]ue to constrained funding, the NSA and NRO Offices of Security indicated that they have suspended the conduct of periodic reinvestigations for contractor employees . . .” does not accurately reflect the situation. In fact, the NSA does not fund its own periodic reinvestigations for contractors; NSA funding was not an issue.<sup>1</sup> To be clear, NSA did not suspend the conduct of periodic reinvestigations for its contractor population. While not speaking on behalf of other agencies, NSA understands that the DSS (Defense Security Service) and NRO (National Reconnaissance Office) had suspended conduct of contractor periodic reinvestigations for a certain period under funding constraints.

(U) Otherwise, Recommendations B(2)(u-c) and B(3) in your Report make specific recommendations concerning NSA. Accordingly, we address each of these Recommendations sequentially:

- (U) B(2)(a). Recommendation that the Director of NSA “[i]n the absence of an overarching DCII policy, evaluate titling and indexing in the DCII the Subjects of all non-criminal investigations conducted by all Agency investigative elements.”

<sup>1</sup> (U) At NSA, the DoD funds contractor (also known as industrial) periodic reinvestigations (PRs).

UNCLASSIFIED

UNCLASSIFIED

*Disagree.* We disagree with applying Recommendation B(2)(a) to the extent that it would apply to security investigations. The DoD-designated repository for investigations of security significance is the Joint Personnel Adjudication System (JPAS). NSA already submits all such cases on DoD contractors to JPAS and to SCATTERED CASTLES (as the IC repository).

- (U) B(2)(b). Recommendation that the Director of NSA "[d]irect [its Office] of Security to develop formal procedures to ensure that reports of investigation into misconduct by contractor personnel are reported to DODCAF" (the DoD Consolidated Adjudication Facility).

*Agree.* Prior to the establishment of the DODCAF in fiscal year 2013, investigations were reported to the Defense Industrial Security Clearance Office. Since then, any case involving contractor misconduct with a national security clearance eligibility nexus has been reported to the DODCAF in accordance with internal standard operating procedures. We will continue to enforce our internal procedures that require the reporting of any derogatory information regarding DoD contractors to the DODCAF.

- (U) B(2)(c). Recommendation that the Director of NSA "[e]nsure that controls are in place to ensure that favorable personnel security adjudicative determinations made with conditions, deviations, or waivers are documented in the 'Exception Information' block of the Subject's SCATTERED CASTLES file."

*Agree.* NSA has provided information to SCATTERED CASTLES since circa 2002. In accordance with ICD 704 (Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information), procedures are already in place to ensure that this information is entered into SCATTERED CASTLES.

- (U) B(3). Recommendation that the NSA IG "work with the Offices of Security of [NSA] to ensure that IG reports of investigation into misconduct by contractor personnel are reported to DODCAF."

*Disagree.* As written, the proposed Recommendation language could impair the independence of the NSA OIG. NSA suggests modifying Recommendation B(3) to clearly state the separate roles for those two organizations, and changing the report to delete the potentially ambiguous "work with" language. Accordingly, we suggest that the Recommendation might state something such as:

"We recommend that the Inspector General of NSA continue to provide IG reports of investigation into substantiated misconduct by contractor personnel (or summaries of these reports) to the NSA Office of Security to enable the NSA Office of Security to report to DODCAF, as required."

However, effective immediately all NSA OIG reports of contractor misconduct received by the ADS&CI will now be disseminated to DODCAF. The ADS&CI is also

UNCLASSIFIED



UNCLASSIFIED

implementing a protocol to ensure that OIG is notified when such reports are forwarded to DODCAF.

(U) We appreciate the opportunity to comment on your Report and investigation.

  
ELIZABETH R. BROOKS  
Chief of Staff

UNCLASSIFIED

# Appendix H

## Defense Human Resources Activity Response to Our Draft Report



DEPARTMENT OF DEFENSE  
DEFENSE HUMAN RESOURCES ACTIVITY  
DEFENSE MANPOWER DATA CENTER  
4800 MARK CENTER DRIVE, SUITE 04E25-01  
ALEXANDRIA, VA 22350-8000

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: An Assessment of Contractor Personnel Security Clearance Processes in the Four Defense Intelligence Agencies (Project No. D2013-DINT01-0009.000)

Thank you for the opportunity to provide comments to the recommendations in the draft report, An Assessment of Contractor Personnel Security Clearance processes in the Four Defense Intelligence Agencies (Project No. D2013-DINT01-0009.000).

The Defense Human Resources Activity and Defense Manpower Data Center comments to the report recommendations are included in the attachment. Please feel free to direct any questions to me, Mary Snavelly-Dixon, at 571-372-0978 or [mary.m.snavelly-dixon.civ@mail.mil](mailto:mary.m.snavelly-dixon.civ@mail.mil).

A handwritten signature in black ink that reads "Mary Snavelly-Dixon".

Mary Snavelly-Dixon  
Director

Attachment:  
As stated

RECOMMENDATIONS  
PROJECT NO. D2013-DINT01-0009.000

**Recommendation B.4:** We recommend that the Director, Defense Human Resources Activity, work with GSA to add EPLS/SAM to the set of databases being accessed by ACES.

Comments: Non-concur. This recommendation is premature since analysis of this data is required to include value of data source in identifying issues impacting federal investigative standards, and determining if the use of that data source meets legal, privacy, and Paperwork Reduction Act requirements. Incorporating the Excluded Parties List/System for Award Management into ACES would also require business analysis, software development, interface development, testing and additional funding/resources to accomplish that work.

**Recommendation E:** We recommend that the Director, Defense Human Resources Activity, develop software to automatically flag the personnel security adjudicative portion of JPAS that a DCII file exists on a specific Subject.

Comments: Concur; however, recommended that this item be modified to develop software to automatically flag the personnel security adjudicative portion of the Case Adjudication Tracking System (CATS) that a Defense Central Index of Investigation (DCII) file exists on a specific subject. CATS, and not the Joint Personnel adjudication System (JPAS), is the primary personnel security system that the DoD Central Adjudication Facility (CAF) uses for adjudication purposes. CATS is one component of the Defense Information System for Security (DISS) family of systems.

**Recommendation A.1:** We recommend that USD (I) Develop and issue an overarching policy governing JPAS operation.

Comments: Recommended that this item be modified to develop and issue an overarching policy governing the System of Record for Personnel Security Clearances, which is currently the Joint Personnel Adjudication System (JPAS). This is to avoid tying the policy to a specific system (i.e. JPAS) since there is a planned transition from JPAS to the Defense Information System for Security (DISS).

# Acronyms and Abbreviations

---

<b>ACES</b>	Automated Continuing Evaluation System
<b>CAF</b>	Clearance Adjudication Facility
<b>CIA</b>	Central Intelligence Agency
<b>DCIS</b>	Defense Criminal Investigative Service
<b>DCII</b>	Defense Central Index of Investigations
<b>DHS</b>	Department of Homeland Security
<b>DIA</b>	Defense Intelligence Agency
<b>DIS</b>	Defense Investigative Service
<b>DCIO</b>	Defense Criminal Investigative Organization
<b>DISCO</b>	Defense Industrial Security Clearance Office
<b>DISCR</b>	Directorate for Industrial Security Clearance Review
<b>DMDC</b>	Defense Manpower Data Center
<b>DNI</b>	Director of National Intelligence
<b>DoE</b>	Department of Energy
<b>DoD</b>	Department of Defense
<b>DODCAF</b>	DoD Consolidated Adjudication Facility
<b>DoDD</b>	Department of Defense Directive
<b>DoDI</b>	Department of Defense Instruction
<b>DOHA</b>	Defense Office of Hearings and Appeals
<b>DoJ</b>	Department of Justice
<b>DSS</b>	Defense Security Service
<b>EO</b>	Executive Order
<b>EPLS</b>	Excluded Parties List System
<b>FBI</b>	Federal Bureau of Investigation
<b>GRS</b>	General Records Schedule
<b>GSA</b>	General Services Administration
<b>IC</b>	Intelligence Community
<b>ICPG</b>	Intelligence Community Policy Guidance
<b>IG</b>	Inspector General
<b>IRTPA</b>	Intelligence Reform and Terrorism Prevention Act of 2004
<b>JPAS</b>	Joint Personnel Adjudication System
<b>NAC</b>	National Agency Check
<b>NARA</b>	National Archives and Records Administration
<b>NGA</b>	National Geospatial-Intelligence Agency
<b>NRO</b>	National Reconnaissance Office
<b>NSA</b>	National Security Agency
<b>OPM</b>	Office of Personnel Management
<b>OMB</b>	Office of Management and Budget
<b>PERSEREC</b>	Defense Personnel Security Research Center
<b>SAM</b>	System for Award Management
<b>SCATTERED</b>	The IC personnel security/access database
<b>CASTLES</b>	
<b>SCI</b>	Sensitive Compartmented Information
<b>SEC</b>	Office of Security, DIA
<b>SSBI</b>	Single Scope Background Investigation
<b>USD(I)</b>	Under Secretary of Defense for Intelligence

**Whistleblower Protection**  
**U.S. DEPARTMENT OF DEFENSE**

*The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD IG Director for Whistleblowing & Transparency. For more information on your rights and remedies against retaliation, go to the Whistleblower webpage at [www.dodig.mil/programs/whistleblower](http://www.dodig.mil/programs/whistleblower).*

**For more information about DoD IG  
reports or activities, please contact us:**

**Congressional Liaison**  
Congressional@dodig.mil; 703.604.8324

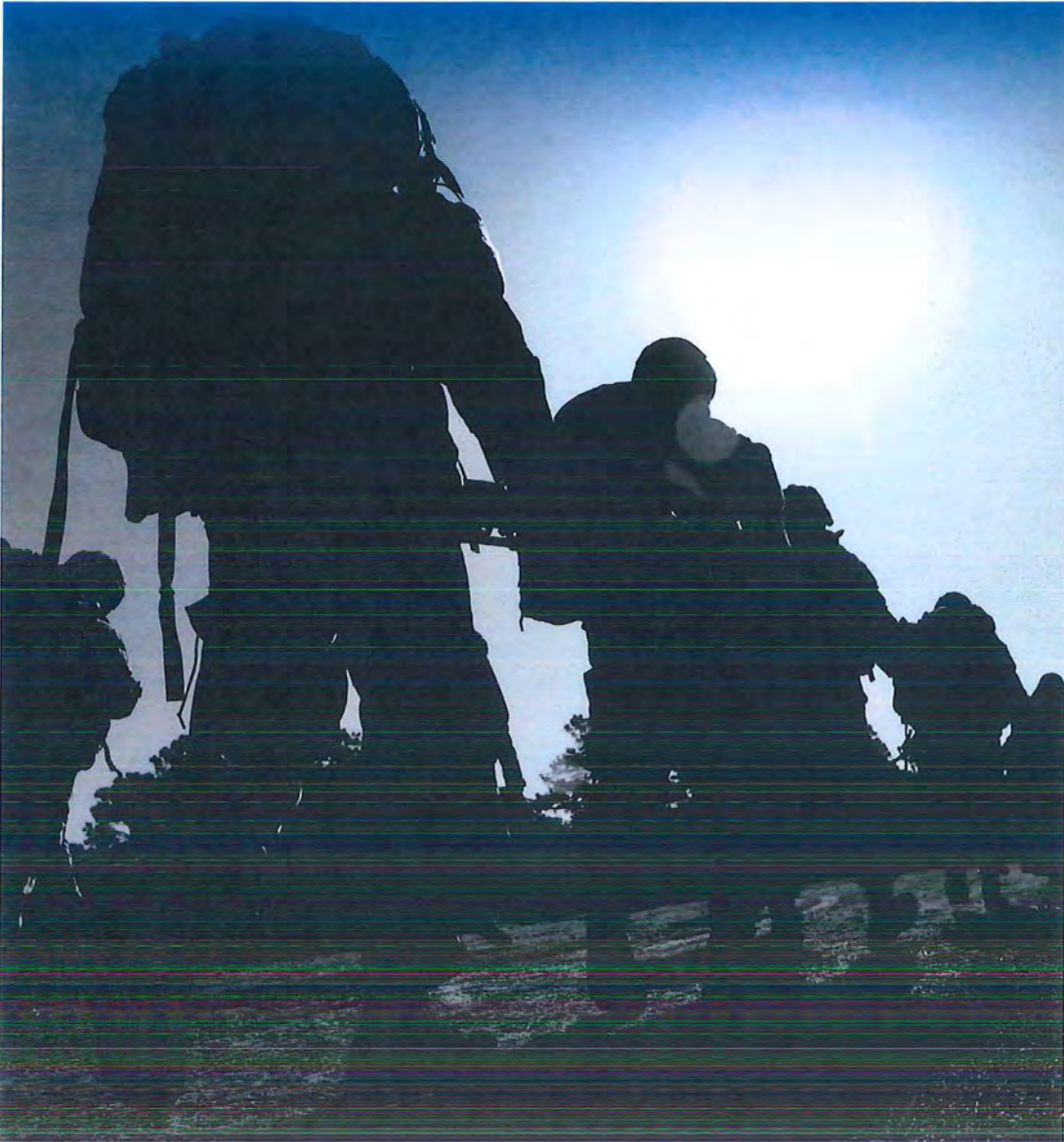
**DoD Hotline**  
800.424.9098

**Media Contact**  
Public.Affairs@dodig.mil; 703.604.8324

**Monthly Update**  
dodigconnect-request@listserve.com

**Reports Mailing List**  
dodig\_report-request@listserve.com

**Twitter**  
twitter.com/DoD\_IG



DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive  
Alexandria, VA 22350-1500  
[www.dodig.mil](http://www.dodig.mil)  
Defense Hotline 1.800.424.9098

