

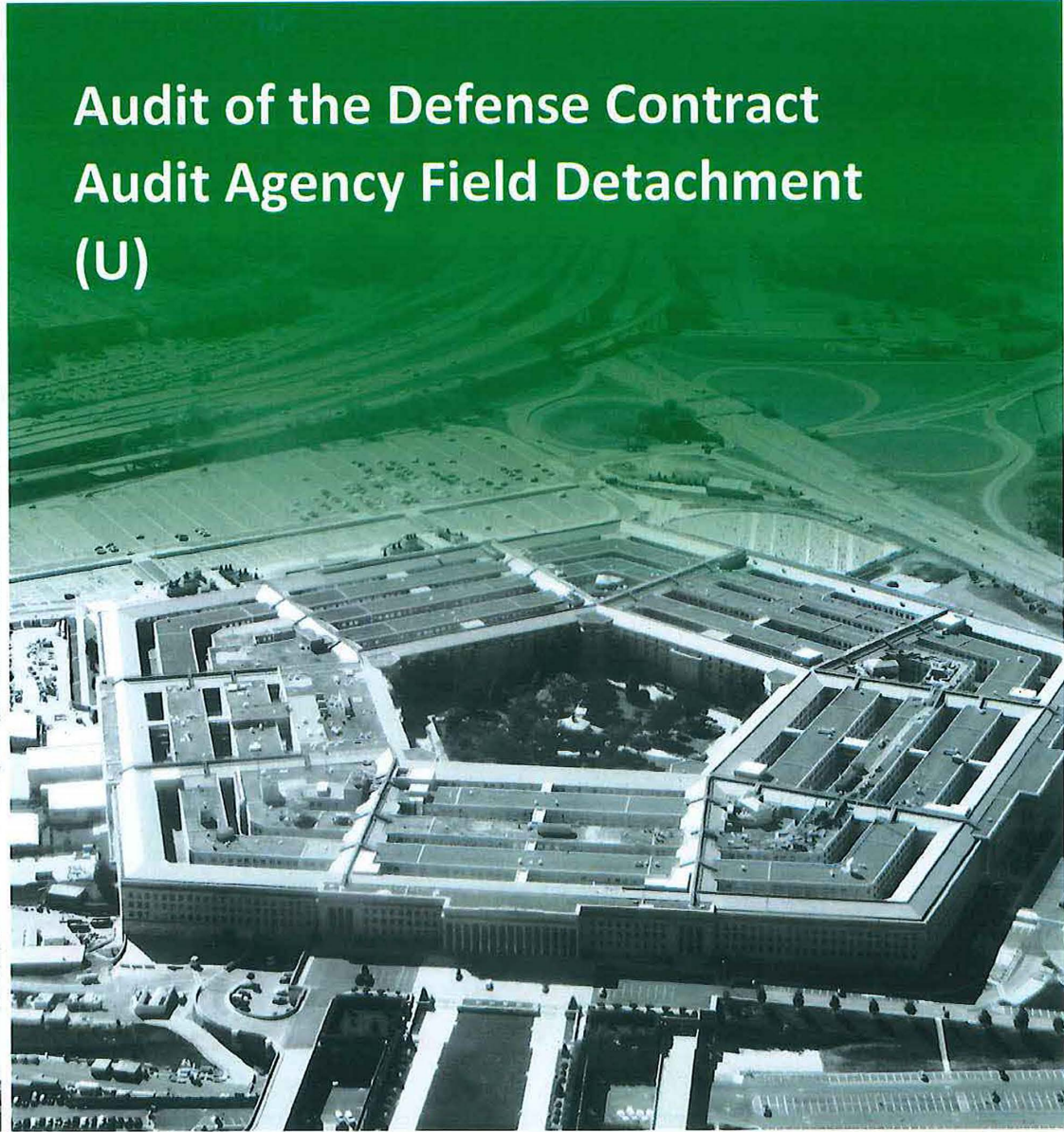
~~FOR OFFICIAL USE ONLY~~



INSPECTOR GENERAL

U.S. Department of Defense

June 14, 2017



Audit of the Defense Contract Audit Agency Field Detachment (U)

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~The document contains information that may be exempt from
mandatory disclosure under the Freedom of Information Act.~~

~~FOR OFFICIAL USE ONLY~~

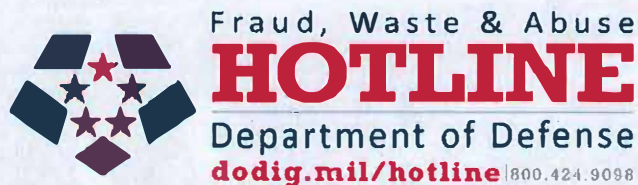
INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense 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.



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



Results in Brief (U)

Audit of the Defense Contract Audit Agency Field Detachment (U)

June 14, 2017 (U)

Objective (U)

(U) We determined whether the Defense Contract Audit Agency (DCAA) Field Detachment (FD) (hereafter referred to as FD) was effectively following DoD directives, policies, and guidelines pertinent to its mission and security. The audit was performed in response to a request from the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office, (hereafter referred to as DoD SAPCO)

Findings (U)

(U//~~FOUO~~) FD did not comply with DoD directives, policies, and guidelines for safeguarding and protecting classified information. For example, FD officials did not:

- (U) have co-utilization agreements for all locations, perform classification reviews of documents containing information extracted from other classified documents, and have detailed records of security incidents;
- (U) maintain a special access program (SAP) access list designating program accesses of the audit staff;
- (U//~~FOUO~~) DoD OIG: (b) (7)(E) [Redacted]
- (U//~~FOUO~~) DoD OIG: (b) (7)(E) [Redacted]

Findings (cont'd) (U)

- (U) complete required security training.

(U//~~FOUO~~) This occurred because FD lacked adequate policies and procedures and did not take adequate corrective actions to address the findings in the May 2012 Staff Assistance Visit conducted by the DoD SAPCO. As a result, FD [Redacted]

(U//~~FOUO~~) In addition, DCAA leadership did not effectively use FD personnel and facilities to support classified and SAP contract audits. This occurred because:

- (U//~~FOUO~~) DCAA leadership placed a priority on non-SAP contract audits;
- (U//~~FOUO~~) FD leadership did not have a process for identifying SAPs to perform audit planning and oversight of classified and SAP contracts; and
- (U//~~FOUO~~) FD did not identify a classified automated information system for conducting classified audit assignments and reports.

(U//~~FOUO~~) As a result, DoD OIG: (b) (7)(E) [Redacted]

Recommendations (U)

(U//~~FOUO~~) In this response, we make 41 recommendations for improvement. Based on comments we received to a draft of this report, we revised the recommendation for the Director, DoD SAPCO to work with the DCAA Security Officer to prioritize security vulnerabilities for remediation and establish timelines for completion. Additionally, we recommend that the DoD SAPCO work with the DCAA Security Officer to correct security vulnerabilities identified in this report.

(U//~~FOUO~~) Among other recommendations, we recommend that the Director, DCAA review and evaluate the leadership and performance of the Director, FD and report any management action taken; develop and implement a formalized program access request process; and take corrective actions on the identified security vulnerabilities.



Results in Brief (U)

Audit of the Defense Contract Audit Agency Field Detachment (U)

Recommendations (cont'd) (U)

(U//~~FOUO~~) We recommend that the FD Regional Director, perform an annual assessment of FD staffing and facility requirements for audit oversight of classified and SAP operations, and establish and implement annual planning and coordination with customer program security officers to identify classified and SAPs.

(U//~~FOUO~~) In addition, we recommend that the DCAA Security Officer correct security deficiencies at FD and develop and implement an incident response plan, including updating policies and procedures, for reporting and investigating FD security incidents.

Management Comments and Our Response (U)

(U//~~FOUO~~) The Security Director, DoD SAPCO addressed all specifics of the recommendation to conduct a risk assessment of all missing FD security incidents and provide a preliminary report within 90 days provided they receive support from DCAA to conduct the risk assessment. Therefore, the recommendation is resolved. We will close the recommendation when we receive the results of the risk assessment.

(U//~~FOUO~~) The Security Director, DoD SAPCO, did not address all specifics of the recommendation to prioritize security

Management Comments and Our Response (cont'd) (U)

(U//~~FOUO~~) vulnerabilities and establish timelines for completion; therefore, the recommendation is unresolved. We will close the recommendation after we verify that ^{DoD OIG: (b) (7)(E)} [REDACTED]

[REDACTED] The Security Director, DoD SAPCO, should provide comments on the final report by July 10, 2017.

(U//~~FOUO~~) The Director, DCAA, addressed all specifics of four recommendations related to the leadership of the FD and implemented corrective actions. As a result, those recommendations are closed. The Director, DCAA, responding for DCAA addressed all specifics of 26 recommendations related to the security operations and oversight of SAPs. Therefore, these recommendations are resolved. These recommendations will be closed when the Director, DCAA, provides, and we review and verify, evidence that the recommendations have been implemented.

(U) The Director, DCAA, responding for DCAA did not address all specifics of the recommendations to:

- (U) complete SAP facility accreditation documentation for the DCAA FD locations; and
- (U) work with the DoD SAPCO to identify all FD personnel SAP accesses and inform the DoD SAPCO of all updates to DoD and ^{DCAA: (b) (7)(E)} [REDACTED]
- (U//~~FOUO~~) ensure SAP contract audits are included in the DCAA annual planning guidance;
- (U//~~FOUO~~) notify all DCAA employees that FD is responsible for performing all audit assignments involving classified or SAP contracts;
- (U//~~FOUO~~) establish an agency wide process requiring auditors to review the DD Form 254, "DoD Contract Security Classification Specification," as part of the program audit plan before performing a review of the contract;



Results in Brief (U)

Audit of the Defense Contract Audit Agency Field Detachment (U)

Management Comments and Our Response (cont'd) (U)

- (U//~~FOUO~~) work with DCAA Security Officer and the DoD SAPCO to designate a group of FD leadership and branch managers to receive access to SAPs to conduct planning and oversight;
- (U) conduct annual planning to identify FD audit oversight efforts for classified and SAP projects;
- (U) reassess the use of regular telework schedules to ensure adequate personnel are available to audit classified and SAP contracts; and,
- (U) acquire and use a classified automated information system for conducting classified audit assignments and reports.

(U) Therefore, the recommendations are unresolved. The Director, DCAA, should provide comments to the final report by July 10, 2017. Please see the recommendations table on the next page.

Recommendations Table (U)

| Management | Recommendations Unresolved | Recommendations Resolved | Recommendations Closed |
|---|------------------------------|---|------------------------|
| (U) Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office | A.1.b | A.1.a | None |
| (U) Director, Defense Contract Audit Agency | B.1.a, B.1.b, B.1.c | A.2.c, A.2.e, A.2.f, B.1.d | A.2.a, A.2.b, A.2.d |
| (U) Field Detachment Regional Director, Defense Contract Audit Agency | B.2.b.1, B.2.b.3, B.2.c | B.2.a, B.2.a.1, B.2.a.2, B.2.a.3, B.2.b, B.2.b.2, B.2.b.4 | None |
| (U) Defense Contract Audit Agency Security Officer | A.3.b, A.3.g, A.3.h, A.3.i.4 | A.3.a, A.3.c, A.3.c.1, A.3.d, A.3.e, A.3.f, A.3.i, A.3.i.1, A.3.i.2, A.3.i.3, A.3.j, A.3.k, A.3.l, A.3.m, A.3.n | None |

(U) Please provide Management Comments by July 10, 2017

(U) The following categories are used to describe agency management's comments to individual recommendations:

- **(U) Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **(U) Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **(U) Closed** – OIG verified that the agreed upon corrective actions were implemented.

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR
ACQUISITION, TECHNOLOGY, AND LOGISTICS
DIRECTOR, DEFENSE CONTRACT AUDIT AGENCY
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTOR, DEPARTMENT OF DEFENSE SPECIAL
ACCESS PROGRAM CENTRAL OFFICE

SUBJECT: Audit of the Defense Contract Audit Agency Field Detachment
(Report No. DODIG-2017-092)

(U//~~FOUO~~) We are providing this report for review and comment. We determined that the Defense Contract Audit Agency Field Detachment did not comply with DoD directives, policies, and guidelines for safeguarding and protecting classified information and did not effectively use Field Detachment personnel and facilities to support special access program contract audits. We conducted this audit in accordance with generally accepted government auditing standards.

(U) We considered management comments on the draft of this report when preparing the final report. DoD Instruction 7650.03 requires that recommendations be resolved promptly. Comments from the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office to Recommendation A.1.a and comments from the Director, Defense Contract Audit Agency to Recommendations A.2.a, A.2.b, A.2.c, A.2.d, A.2.e, A.2.f, A.3.a, A.3.c, A.3.c.1, A.3.d, A.3.e, A.3.f, A.3.i, A.3.i.1, A.3.i.2, A.3.i.3, A.3.j, A.3.k, A.3.l, A.3.m, A.3.n, B.1.d, B.2.a, B.2.a.1, B.2.a.2, B.2.a.3, B.2.b, B.2.b.2, and B.2.b.4 addressed all specifics of the recommendations and conformed to the requirements of DoD Instruction 7650.03.

(U) As a result of management comments, we revised recommendation A.1.b, directed to the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office. Comments from the Director, Defense Contract Audit Agency, to Recommendations A.3.b, A.3.g, A.3.h, A.3.i.4, B.1.a, B.1.b, B.1.c, B.2.b.1, B.2.b.3, and B.2.c did not address all specifics of the recommendations. Therefore, the recommendations are unresolved. The Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office and the Director, Defense Contract Audit Agency should provide additional comments to Recommendations A.1.b and A.3.b, A.3.g, A.3.h, A.3.i.4, B.1.a, B.1.b, B.1.c, B.2.b.1, B.2.b.3, and B.2.c, respectively, by June 10, 2017.

(U) We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-7331 ~~DoD OIG: (b) (6)~~

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operation

(U) Contents

| | |
|---|-----------|
| (U) Introduction | 1 |
| (U) Objective..... | 1 |
| (U) Background..... | 1 |
| (U) Review of Internal Controls..... | 2 |
| | |
| (U) Finding A FD Did Not Comply With DoD Security Guidance | 4 |
| (U) DCAA: (b) (7)(E) | 4 |
| (U) FD Workforce Program Accesses..... | 9 |
| (U) Conclusion..... | 16 |
| (U) Management Comments on the Finding and Our Response..... | 17 |
| (U) Recommendations, Management Comments, and Our Response..... | 19 |
| | |
| (U) Finding B FD Did Not Effectively Use Personnel and Facilities to Support SAP Contract Audits | 28 |
| (U) Management of Field Detachment Personnel and Facilities to Support Classified and SAP Audits..... | 28 |
| (U) FD Oversight..... | 31 |
| (U) Conclusion..... | 33 |
| (U) Management Comments on the Finding and Our Response..... | 33 |
| (U) Recommendations, Management Comments, and Our Response..... | 35 |
| | |
| (U) Appendix | |
| (U) Scope and Methodology..... | 44 |
| (U) Use of Computer-Processed Data | 45 |
| (U) Prior Coverage | 45 |
| | |
| (U) Management Comments | 46 |
| (U) Security Director, DoD Special Access Program Central Office..... | 44 |
| (U) Director, Defense Contract Audit Agency..... | 44 |
| | |
| (U) Acronyms and Abbreviations | 65 |

Introduction (U)

Objective (U)

(U) The audit objective was to determine whether the Defense Contract Audit Agency (DCAA) Field Detachment (FD) was effectively following DoD directives, policies, and guidelines pertinent to its mission and security. The audit was performed in response to a request from the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office (hereafter referred to as DoD SAPCO). The Director, DoD SAPCO requested that the DoD Office of Inspector General conduct a comprehensive evaluation of the management and security processes at the DCAA FD. See the Appendix for the scope and methodology used to meet the audit objective.

Background (U)

(U) The DCAA FD (hereafter referred to as FD), a component of DCAA, was established in 1958 as a component of the Air Force Audit Agency to provide contracting support for Airborne Reconnaissance Programs. However, in 1960 FD was expanded with the creation of the National Reconnaissance Office, and in 1968 was reassigned to DCAA.

(U) In accordance with DoD Directive 5205.07,¹ FD conducts audits of DoD SAP contracts, and is responsible for the overall planning, management, and execution of all DCAA contract audits of sensitive compartmented information and SAPs. FD supports NRO: (b) (3), 10 USC § 424 contractor sites, with NRO: (b) (3), 10 USC § 424 of that support provided in National Reconnaissance Office accredited facilities.

(U) As of November 19, 2015, FD consisted of a regional office, DCAA field audit offices (FAOs), DCAA sub offices, and DCAA financial liaison advisors.² FD is comprised of approximately 450 personnel providing audit and financial advisory support services to the National Reconnaissance Office's NRO: (b) (3), 10 USC § 424 contracting officers. The FD regional office, located in DoD OIG: (b) (7)(E) Virginia, provides oversight and direction to all FD

¹ (U) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010.

² (U) The FD regional office is the FD's headquarters office, which falls under the DCAA headquarters. The field audit offices are also known as branch offices. The financial liaison advisors reside in FD facilities; however, the advisors report to DCAA headquarters.

(U) operations and assignments. In addition, the regional office manages and supports audit work performed by the field and sub offices by providing senior management oversight, human resources, technical programs, security, budget, information technology help desk, and special programs assistance.

(U) FD provides various services, including annual incurred cost audits; mandatory annual audit requirement [MAAR] 6 (labor costs, personnel checks, and interviews) and mandatory annual audit requirement [MAAR] 13 (purchase existence and consumption) reviews; forward pricing audits; financial liaison assistance; and interim, provisional, and billing audits.

Criteria (U)

(U) DoD Directive 5205.07 contains policy and responsibilities for the oversight and management of all DoD SAPs. DoD SAPCO is responsible for advising and assisting the Secretary of Defense (SecDef) and Deputy SecDef with governance, management, and oversight of DoD SAPs. DoD SAPCO is also the primary liaison to executive branch agencies and the Congress on all SAP issues.

(U) DoD Instruction 5205.11³ establishes and implements policy, assigns responsibilities, and updates and prescribes procedures for the management, administration, and oversight of all DoD SAPs.

(U) DoD Instruction 5000.64⁴ establishes accountability and management policy for DoD-owned equipment and other accountable property.

Review of Internal Controls (U)

(U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. As discussed in the report, we identified internal control weaknesses in the program access request (PAR) process.

³ (U) DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," February 6, 2013

⁴ (U) DoD Instruction 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property," May 19, 2011

(U) Specifically, FD did not initiate, approve, debrief, and maintain personnel SAP accesses. In addition, FD did not have up-to-date security standard operating procedures. We will provide a copy of our audit report to the senior official responsible for internal controls in DCAA and the Under Secretary of Defense for Acquisition, Technology, and Logistics.

Finding A (U)

FD Did Not Comply With DoD Security Guidance (U)

(U//~~FOUO~~) FD did not comply with DoD directives, policies, and guidelines for the safeguarding and protection of classified and SAP information. For example, FD officials did not:

- (U) have co-utilization agreements for all FD locations,⁵ perform classification reviews of documents containing information extracted from other classified documents, and maintain detailed records of security incidents;
- (U) maintain a SAP access list designating program accesses of the audit staff;
- (U) ~~DoD OIG (b) (7)(E)~~
- (U//~~FOUO~~) ~~DoD OIG (b) (7)(E)~~
- (U) complete required security training.

(U//~~FOUO~~) This occurred because FD lacked adequate policies and procedures and FD leadership did not provide effective oversight of security-related issues, including taking adequate corrective actions to address the findings in the May 2012 Staff Assistance Visit conducted by the DoD SAPCO. ~~DoD OIG (b) (7)(E)~~

~~DCAA (b) (7)(E)~~

(U)

(U) FD did not comply with DoD directives, policies, and guidelines for safeguarding and protecting classified information. For example, FD officials did not have co-utilization

⁵ (U) A co-utilization agreement documents areas of authorities and responsibilities between cognizant security offices when they share the same SAP facilities.

⁶ (U) According to DoD Manual 5205.07, volume 1, "Special Access Program (SAP) Security Manual General Procedures," ~~DCAA (b) (7)(E)~~

agreements, perform classification reviews, and have detailed records of security incidents.

Co-Utilization Agreements (U)

(U//~~FOUO~~) FD did not have co-utilization agreements for all locations. DoD Manual 5205.07, volume 1, states that co-utilization agreements are required when multiple SAP programs are stored together and worked on in the same facility.⁷ At the DoD OIG: (b) (7)(F) and NRO: (b) (3), 10 USC 4124 Branch Offices we identified that FD co-mingled SAP information from different SAPs in the same safe drawers. According to FD Security officials, co-utilization agreements did not exist for DoD OIG: DCAA: (b) (7)(E) (b) (7)(E). Therefore, the Branch offices violated DoD guidance by storing multiple programs in the same safe drawers without the co-utilization agreements. The DCAA Security Officer needs to identify and complete all required co-utilization agreements in accordance with DoD Manual 5205.07, volume 1.

Security Classification Reviews (U)

(U) FD personnel did not request that customer program security officers perform classification reviews of documents containing information extracted from other classified documents. According to DoD Manual 5200.01, volume 1, "classification as a result of compilation⁸ requires an original classification decision by an authorized original classification authority⁹ or classification guidance issued by an original classification authority (e.g., a security classification guide)."¹⁰ However, FD classification guidance was not updated to reflect the most recent security guidance and did not require classification reviews. In addition, FD personnel stated that security classification guides were not always provided by the audited customer. Instead of requesting a classification review from the customer program security officers, the FD supervisor conducted the classification reviews. For example, an FD supervisor located at FD headquarters stated that it was the supervisors' responsibility to conduct a classification review. The FD supervisor might not be able to identify all instances

⁷ (U) DoD Manual 5205.07, volume 1, "Special Access Program (SAP) Security Manual: General Procedures," June 18, 2015.

⁸ (U) Classification as a result of compilation occurs when unclassified elements of information are combined to reveal classified information, or when classified elements combine to reveal information at a higher classification level than the individual elements.

⁹ (U) Original classification Authority is an individual authorized in writing to originally classify information (i.e., to classify information in the first instance). The responsible OCA shall issue security classification guidance for each program, project, or mission involving classified information. The classification guidance may be in the form of a security classification or declassification guide.

¹⁰ (U) DoD Manual 5200.01, volume 1, "DoD Information Security Program, Overview, Classification, and Declassification," February 24, 2012.

where compilation would result in classified information, which increases the risk of an unauthorized disclosure of classified information due to compilation. DCAA Security Officer needs to update internal guidance to require classification reviews from the program security officer for audit work derived from classified information.

Security Incident Reporting (U)

(U) FD did not have detailed records of security incidents in accordance with DoD guidance. Specifically, FD Instruction 5210.16 did not reference DoD Manual 5205.07, volume 1.¹¹ For example, FD policy does not require FD Security to notify and report security violations to the Government program manager and the cognizant authority SAPCO. The FD policy did not include the requirement to report actual or potential compromises involving DoD SAPs to DoD SAPCO. FD did not have documentation of security incidents and corrective action taken in response to the incidents. Therefore, FD did not have a record of FD personnel:

- (U//~~FOUO~~) DoD OIG: (b) (7)(E) [REDACTED]
- (U//~~FOUO~~) with a pattern of security incidents, which may lead to a more serious violation; or
- (U//~~FOUO~~) required corrective actions as a result of the incident.

Missing and Incomplete Security Incident Data (U)

(U//~~FOUO~~) FD did not have detailed records or reports for security incidents that occurred before January 2015. Security incident data was stored in the DoD OIG: (b) (7)(E) [REDACTED] a classified closed network FD used to conduct work on unclassified, classified, and SAP audits.¹² However, DoD OIG: (b) [REDACTED] was terminated on August 14, 2014, and detailed information for security incidents that occurred before January 2015 was lost. The only information available was a security incident log beginning in October 2014; however, that data was incomplete. Further, although FD has some security incident data for 2015 and 2016, that data was incomplete. For example, the log indicated that FD personnel brought unauthorized electronic devices into the sensitive compartmented information facility (SCIF); however, the log did not

¹¹ (U) FD Instruction 5210.16, "Security Incidents," December 22, 2009.

¹² (U) A closed network is telecommunications network used for a specific purpose, such as a payment system, which access is restricted.

contain the date of the incident, the date reported, or any required corrective actions. According to one of the FD general SAP Security Officers,¹³ a prior security specialist did not always close out or document all incidents. Further, the ~~NRO: (b) (3), 10 USC 8424~~ and ~~DoD OIG: (b) (7)(E)~~ FAOs did not have any security incident logs.

Inadequate Restrictions for FD Security Incident Logs (U)

(U) At the time of our review, FD did not restrict access to its security incident logs. FD security incident logs are stored ~~DoD OIG: (b) (7)(E)~~ accessible by selected FD security ~~DoD OIG: (b) (7)(E)~~. As a result, ~~DoD OIG: (b) (7)(E)~~

~~DoD OIG: (b) (7)(E)~~ The DCAA Security Officer should develop and implement an incident response plan, including updated policies and procedures, for reporting, tracking, and investigating FD security incidents. The incident log should be restricted ~~DoD OIG: (b) (7)(E)~~.

Inappropriate Access and Storage of SAP Material (U)

(U//~~FOUO~~) ~~DoD OIG: (b) (7)(E)~~ For example, FD personnel at the ~~NRO: (b) (3), 10 USC 8424~~ and ~~DoD OIG: (b) (7)(E)~~ Branch Offices ~~DoD OIG: (b) (7)(E)~~

~~DoD OIG: (b) (7)(E)~~ In addition, FD personnel did not complete the Standard Form 700, "Security Container Information" (SF 700),¹⁴ in accordance with DoD Manual 5200.01, volume 3.¹⁵ Specifically, FD personnel:

- (U) did not update the ~~NRO: (b) (3), 10 USC 8424~~ and ~~DoD OIG: (b) (7)(E)~~ Branch Office SF 700s with the current employee contact information;
- (U) did not classify the ~~DoD OIG: (b) (7)(E)~~ Branch sub office SF 700s at the highest level of information maintained in the two security containers located in that office;

¹³ (U) The general SAP security officer is a government official appointed in writing at a SAP facility or organization by the Director or program manager to provide security administration and management. The general SAP security officer receives SAP guidance from the program security officer.

¹⁴ (U) The SF 700 is a record for each container, vault, or secure room door that is used for storing classified information.

¹⁵ (U) DoD Manual 5200.01, volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012 (Incorporating Change 2, March 19, 2013).

- (U) did not document and maintain a SF 700 in a safe that contained classified documents at a DoD OIG: (b) (7)(E) Branch sub-office; and
- (U) stored a SF 700 inside a DoD OIG: (b) (7)(E) Branch sub-office security container rather than having the combination stored separately.

(U) FD personnel who no longer worked in FAOs were listed as contact points for the SAP information stored in the safe, and FD security containers had information classified higher than authorized. On October 7, 2016, DCAA leadership provided us a memorandum requesting that FD personnel take immediate corrective actions concerning the inappropriate access to classified material at the FAOs. The memorandum also required branch managers to report on the corrective actions taken. However, DCAA leadership did not provide documentation supporting that corrective action was actually taken. To ensure that corrective action was taken in response to the memorandum, the DCAA Security Officer needs to validate that access to SAP information, DCAA: (b) (7)(E) [REDACTED]. In addition, the DCAA Security Officer should ensure that FD completes SF 700s with all required information in accordance with DoD guidance.

Authorized Access Lists and Visitor Logs (U)

(U) FD did not have authorized access lists and visitor logs for its computer server rooms. National Institute of Standards and Technology Special Publication 800-53, Revision 4, requires organizations to select and specify security controls for information systems, including the implementation of adequate physical authorization and access controls for information systems.¹⁶ The use of a visitor log minimizes the opportunity for unauthorized access to the FD computer server rooms. DCAA Security Officer needs to implement the use of authorized access lists and visitor logs in all DCAA computer server rooms.

(U) Appointment Letters

(U) FD did not formally appoint its general SAP security officers in accordance with DoD Manual 5205.07. The Manual states that general SAP security officers will be designated to support SAPs. The appointment letters formally designate individuals and identify their roles and responsibilities as general SAP security officers. Without

¹⁶ (U) National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," 2013 (incorporates updates as of January 22, 2015).

this formal designation the general SAP security officers may not be aware of their roles and responsibilities. For example the general SAP security officers:

- (U) did not formally debrief individuals when access to SAP information was no longer required;
- (U) did not perform classification reviews; and
- (U) did not receive their required Defense Security Service SAP training.

(U) The DCAA Security Officer needs to formally appoint general SAP security officers in writing.

Facility Accreditation (U)

(U) FD did not maintain facility accreditation documentation at the FAOs we visited where personnel were conducting SAP audits. DoD Manual 5205.07, volume 3, requires facility accreditation documentation to be retained at each site.¹⁷ The FAO facilities were accredited as SCIFs, not as SAP facilities. Therefore, FD personnel should not have performed SAP audits in these facilities because those FAO facilities did not have the DCAA (b) (7)(E) [REDACTED]. As a result, NRO: (b) (3), 10 USC [REDACTED] Branch Office personnel DoD OIG: (b) (7)(E) [REDACTED] [REDACTED]

(U) In November 2015, FD leadership initiated an internal business process implementation team (BPIT). One BPIT responsibility included identifying and gathering required accreditation documentation. However, the BPIT did not assess the adequacy of DCAA: (b) (7)(E) [REDACTED] controls at each facility DCAA: (b) (7)(E) [REDACTED] DCAA: (b) (7)(E) [REDACTED]. The DCAA Security Officer should complete SAP facility accreditation documentation DCAA: (b) (7)(E) [REDACTED] for the FD locations, in accordance with DoD guidance.

FD Workforce Program Accesses (U)

(U) FD did not have knowledge of SAP accesses and did not maintain a SAP access list designating who of its audit staff had program access. In addition, FD did not have a formal PAR process to identify, initiate, approve, maintain, and debrief personnel.

¹⁷ (U) DoD Manual 5205.07, volume 3, "Special Access Program (SAP) Security Manual: Physical Security," September 21, 2015 (April 23, 2015).

SAP Accesses (U)

(U) FD leadership was not aware of FD workforce's SAP accesses and did not maintain a SAP access list designating program accesses of the audit staff. DoD Manual 5205.07, volume 2, states that "records must be maintained within a personnel security file for each SAP-accessed individual."¹⁸ The records include PARs and transfer access approvals. However, FD security did not have an accurate record of personnel authorized SAP access. In addition, the BPIT did not include the involvement of DoD SAPCO and customer program security officers to assist in identifying the individuals authorized for SAP accesses.

(U//~~FOUO~~) FD leadership also directed the BPIT to identify the total number of personnel SAP accesses and determine if any personnel should be debriefed. The BPIT identified questionable briefings at ~~DoD~~ ~~OIG:~~ ~~(b) (7)~~ FAOs.¹⁹ For example, ~~DoD~~ ~~OIG:~~ ~~(b) (7)~~ former employees were never debriefed from SAPs and ~~DoD~~ ~~OIG:~~ ~~(b) (7)~~ former employees were never debriefed from sensitive compartmented information. However, the BPIT did not identify all accesses because the Joint Access Database Environment (JADE) the team used does not include all non-DoD SAP accesses.²⁰ The BPIT team also relied on FD personnel interviews to identify SAP accesses because FD Security did not document and maintain the information in accordance with the DoD guidance. Without the involvement of DoD SAPCO or the program security officers, the BPIT does not have full knowledge of personnel SAP accesses.²¹ As a result, the total number of personnel that have authorized access to SAPs is unknown. The DoD SAPCO and program security officers are responsible for the oversight and management of SAPs and should have been involved in verifying the accuracy of SAP accesses.

(U) In addition to not identifying all of the personnel accesses, the documents the BPIT created to determine and identify accesses did not meet DoD requirements. The requirements state that the general SAP security officers will maintain an up-to-date separate program access roster for each program resident within a SAP facility.²² The

¹⁸ (U) DoD Manual 5205.07, volume 2, "Special Access Program (SAP) Security Manual: Personnel Security," November 24, 2015.

¹⁹ (U) Questionable briefings include FD personnel that are currently briefed to SAPs that no longer need access.

²⁰ (U) The Joint Access Database Environment (JADE) only manages the Office of the Secretary of Defense SAP cleared personnel and programs.

²¹ (U) The program security officer is a government official appointed in writing by the appropriate cognizant authority SAPCO or designee, and is responsible for executing oversight and implementation of SAP security requirements for a specific SAP or group of SAPs, or geographically assigned locations.

²² (U) At the time of the audit the Joint Air Force-Army-Navy (JAFAN) 6/O Manual, "Special Access Program Security Manual - Revision 1," May 29, 2008, was the governing requirement.

manual also states that access rosters will be properly protected and maintained, and be continually reviewed and reconciled for discrepancies. The roster should also contain the name of the individual, position, billet number if applicable, level of access, social security number, and security clearance information.

(U//~~FOUO~~) Additionally, the BPIT did not have controls in place to prevent the [DoD OIG: (b) (7)(E)]. For example, the BPIT did not implement security measures to [DoD OIG: (b) (7)(E)].

[DoD OIG: (b) (7)(E)] In addition, policies were not in place to define responsibilities for maintaining, updating, and coordinating the information with the DCAA Security Division and DoD SAPCO. As a result, [DoD OIG: (b) (7)(E)].

[DoD OIG: (b) (7)(E)] The DCAA Security Officer needs to identify all SAP access by employee and coordinate that information with DOD SAPCO and, develop and maintain a SAP master list with adequate security controls to restrict unauthorized access.

Program Access Request Process (U)

(U) FD did not have a formal PAR process for requesting, initiating, approving, debriefing, and maintaining personnel SAP accesses and [DoD OIG: (b) (7)(E)].

[DoD OIG: (b) (7)(E)] According to FD Instruction 5205.35, "request for program accesses will be initiated by or coordinated with FD Division Chiefs and FAO Managers, and will be monitored by the FD Program Security Manager."²³ The FD Regional Director stated that the process for approving PARs was revised and she is now responsible for approving all PARs.²⁴ She revised the process to [DoD OIG: (b) (7)(E)].

[DoD OIG: (b) (7)(E)] However, FAOs are not consistent in how the offices request and receive approval to access SAPs. For example, personnel at the [DoD OIG: (b) (7)(E)] Branch Office were coordinating PARs directly with the customer program security officers without the knowledge, involvement, or consent of FD leadership or security personnel. As a result, FD security was unaware of SAP accesses [DCAA: (b) (7)(E)].

(U//~~FOUO~~) DoD Instruction 5205.11 states that granting access to a SAP will be based solely on a determination that the individuals have the need-to-know, the requisite

²³ (U) FD Instruction 5205.35, "Program Access Request and Briefings," January 9, 2012.

²⁴ (U) On November 26, 2016, we were notified that the FD Regional Director was reassigned and is no longer the FD Regional Director.

security clearance, and will clearly and materially contribute to the oversight of the program. For example, we identified individuals at the NRO: (b) (3), 10 USC 6424 Branch Office with access to SAPs who were not actively working on them. Those individuals did not have a valid need-to-know and are not materially contributing to the oversight of the SAP. Therefore the individuals should be de-briefed from the programs. The Director, DCAA and DCAA Security Division need to develop and implement a formalized automated process to request, initiate, approve, debrief, and maintain personnel SAP accesses. This process should be coordinated with DoD SAPCO and customer program security officers to make sure FD have accurate and current information.

Document and Property Accountability (U)

(U//~~FOUO~~) FD did not follow DoD guidance for accountability of Top Secret and SAP documents. In addition, FD did not maintain accurate accountability of property.

Document Accountability and Responsibilities (U)

(U//~~FOUO~~) FD did not follow DoD guidance for the accountability of Top Secret and SAP documents and the designated Top Secret Control Officers (TSCO) and alternate TSCOs DoD OIG: (b) (7)(E). DoD Manual 5205.07, volume 1, requires a separate accountability system for all SAP information. It establishes the minimum required information for an accountability log and the requirement to conduct a 100-percent inventory annually. However, FD did not have separate accountability systems for collateral Top Secret and SAP information. Instead, the TSCOs and their alternate TSCOs only maintained one accountability log for classified documents, including Top Secret and SAP. In addition, the FAOs were not following FD internal security standard operating procedures requiring accountability of all hardcopy documents classified above Unclassified//For Official Use Only and Handle via Special Access Channels Only. Based on a review of documents in the safes, we identified classified documents that were not logged for accountability. For example, the DoD OIG: (b) (7)(E) Branch Office safes contained documents above Unclassified//For Official Use Only that were not logged and accounted for. In addition, the FD internal guidance for accountability was outdated and not in accordance with DoD policy. For example, FD Instruction 5210.5 did not include the guidance in DoD Manual 5205.07, volume 1, requiring a separate accountability system for collateral Top

Secret and SAP information.²⁵ The DCAA Agency Security Officer needs to update internal guidance for accountability in accordance with DoD policy.

(U//~~FOUO~~) Accountability control logs at the FAOs did not contain the minimum information required by the DoD Manual 5205.07, volume 1. DoD Manual 5205.07, volume 1, requires the classification, originator of the item, title and description, custodian, custodian assigned, date of product, control numbers maintained in consecutive sequence, page count, and internal, disposition and date, destruction date, and external receipt records be included in the log. For example, at the ~~DoD OIG: (b) (7)(E)~~ Branch Office the control logs did not contain the originators of the document. Also, the titles and descriptions of documents were vague, page counts were incorrect, overall classification of the information was mismarked, and control numbers were not maintained in consecutive sequence. The DCAA Agency Security Officer needs to develop a standard accountability log for FD designated accountable material, collateral Top Secret, and SAP material that contain the required information.

(U//~~FOUO~~)

~~DoD OIG: (b) (7)(E)~~

Property Accountability (U)

(U//~~FOUO~~) FD did not maintain accurate accountability of its equipment. DoD Instruction 5000.64 requires that FD maintain 100-percent accountability of its equipment at all times. However, property accountability personnel at the ~~DoD OIG: (b) (7)(E)~~ Branch Office did not have administrative authority from January 2015 to February 2016 to update their property records. We identified errors in those property records, including a lack of equipment location, variations in equipment identification numbers (DCAA identification number, serial number, part number), and empty data cells (location and personnel assignment data).

²⁵ (U) FD Instruction 5210.5, "Document Control Procedures," February 1, 2012.

(U//~~FOUO~~) We reviewed the ~~DoD OIG: (b) (7)(E)~~ Branch Office property file consisting of 490 pieces of equipment and noted that 92 listings did not include property locations. In addition, at the ~~DoD OIG: (b) (7)(E)~~ Branch Office we conducted a non-statistical sample of accountable property to inventory and observed that the equipment locations were inaccurate. We also identified that equipment was moved to other field offices without notifying the property accountability personnel. As a result, FD property officials do not have accountability of all equipment. The Director, DCAA needs to make certain all property accountability officials are authorized to update property accountability files.

Properly Disposing of Accountable Property (U)

(U) The FD did not properly manage and dispose of its damaged and excess property. DoD Instruction 5000.64 states that "all persons entrusted with the management of Government property shall be responsible for the disposal or disposition of all property to include directing the appropriate disposition of property." We identified excess, damaged, and unused equipment at the following FAOs:

- (U) ~~NRO: (b) (3), 10 USC 474~~ Branch Office;
- (U) ~~DoD OIG: (b) (7)(E)~~ Branch Office;
- (U) ~~DoD OIG: (b) (7)(E)~~ Branch Office; and
- (U) ~~DoD OIG: (b) (7)(E)~~ Branch Office.

(U//~~FOUO~~) The FAOs also did not properly dispose of excess ~~DoD OIG: (b) (7)(E)~~ equipment and other accountable property. For example, at the ~~NRO: (b) (3), 10 USC 474~~ Branch Office we observed ~~DoD OIG: (b) (7)(E)~~ equipment and other damaged property stored in the server room, hallways, and in unused work spaces ~~DoD OIG: (b) (7)(E)~~ was terminated in August 2014; however, FD leadership has allowed excess equipment to remain in the FAOs for more than two years. DCAA needs to promptly dispose of damaged and excess equipment.

(U) Security Training

(U//~~FOUO~~) FD personnel did not complete required DoD security training. DoD Directive 5205.07 requires DCAA to maintain a designated cadre of SAP trained personnel to provide audit support of DoD contracts. According to DoD guidance, an individual is considered SAP trained after that individual completes the Defense Security Service Academy SAP Orientation Course. Although FD leadership did not maintain training records before the termination of ~~DoD OIG: (b) (7)(E)~~ we identified FD personnel,

including a general SAP security officer, who did not complete the required orientation course.

(U//~~FOUO~~) FD personnel also did not complete mandatory annual SAP awareness training. We reviewed a non-statistical sample of ^{fDCA} records for FY 2016 and determined that 100 percent of the sampled FD employees did not complete mandatory annual SAP awareness training, required by DoD Manual 5205.07, volume 1. According to the FD Director of Security, mandatory annual SAP awareness training had not been conducted for at least two years because DCAA leadership decided to offer generic information security training instead of the tailored FD training. DoD Manual 5205.07, volume 1, states that the general SAP security officer is responsible "to establish, conduct, and document initial, event-driven, and refresher training for all SAP-accessed individuals." Additionally, the FD Regional Director was not aware that Defense Security Service SAP initial and refresher training was a requirement. Further, the FD Annual Security Refresher training provided to FD personnel did not include the mandatory topics required by the DoD 5205.07, volume 1. For example, the training did not include any modules on the protection of classified relationships, operations security, program threats, and types and categories of SAPs. Therefore, FD employees are not adequately prepared to protect SAP information and might be unaware of the procedures to address security incidents in their offices. The DCAA Security Officer should make sure FD has an adequately trained SAP workforce and that mandatory SAP training is annually completed and tracked.

Corrective Actions Not Taken to Address Staff Assistance Visit Deficiencies (U)

(U//~~FOUO~~) FD leadership did not provide effective oversight of security-related issues, including taking corrective actions to address deficiencies identified during the DoD SAPCO Staff Assistance Visit formal compliance inspection in May 2012. The Staff Assistance Visit identified seven areas of concern in FD. We identified similar security deficiencies because FD had not taken corrective action in response to the DoD SAPCO recommendations, including:

- (U) creating an accountability system for Top Secret and SAP holdings, including computer media;
- (U) following up and closing out 27 open security incidents or violations;

- (U) updating the FD security standard operating procedures in accordance with the DoD Manual 5205.07, volume 1;
- (U) providing the FD TSCOs and alternates with access to all information to properly account for the material; and
- (U) documenting and validating the completion of security training.

(U) The FD Director of Security stated that she was not aware that the Staff Assistance Visit recommendations were part of a formal compliance inspection.²⁶ In addition, the FD Regional Director stated that she was not aware:

- (U) of any corrective action taken by the FD Director of Security in response to the recommendations, and
- (U//~~FOUO~~) of the specific 27 open security violations or incidents identified in the Staff Assistance Visit.

(U) The Director, DCAA needs to review and evaluate the leadership and performance of the Director, FD and report on what, if any management action has been taken; designate FD security duties to a qualified security official, and implement the recommendations in the 2012 DoD SAPCO Staff Assistance Visit report. The DoD SAPCO, in conjunction with the DCAA Security Division, should conduct a risk assessment on all lost security incident information. The DoD SAPCO should also work with the DCAA Security Division to prioritize security vulnerabilities for remediation and establish timelines for completion.

Conclusion (U)

(U//~~FOUO~~) The FD Director must take immediate corrective actions in the FD security program to reduce its risk of ~~DCAA: (b) (7)(E)~~. DoD establishes requirements, restrictions, and other safeguards necessary to prevent the unauthorized disclosure of SAP information and necessary to control disclosure of classified information. However, ~~DoD OIG: (b) (7)(E)~~

~~_____~~
~~_____~~ In addition, FD personnel were unaware of potential violations and infractions ~~DCAA: (b) (7)(E)~~. We acknowledge

²⁶ (U) On February 20, 2016, ~~DoD OIG: (b) (6)~~ ~~_____~~ by the Director, DCAA.

the efforts made by the BPIT team to identify facility accreditation documentation and determine SAP accesses. DCAA (b) (7)(E)

[REDACTED]. The FD Director needs to work with DoD SAPCO; the Director, DCAA; and the DCAA Security Officer to address the specific recommendations in this report.

Management Comments on the Finding and Our Response (U)

Management Comments on FD's Compliance With Security Policies (U)

(U//~~FOUO~~) The Director, DCAA, did not agree with certain parts of the finding, specifically, that FD did not comply with any DoD directives, policies, and guidelines for safeguarding and protecting classified information and that FD policies and procedures that incorporate the DoD guidance was available for review. The Director also did not agree that classification reviews of documents containing information extracted from other classified documents is required, stating that FD personnel are derivative classifiers and follow DoD Manual 5200.01, volume 1. The Director also did not agree that FD officials did not DoD OIG (b) (7)(E)

[REDACTED] Further, the Director did not agree with the conclusion DCAA (b) (7)(E), stating that the report provided no evidence, no recommendation, and no examples in the report that FD DCAA (b) (7)(E)

[REDACTED] However, the Director added that based on the audit, DCAA is aware of the areas where improvement is required. Also, the Director added that some modifications to the wording in the report would resolve DCAA concerns with the finding.

(U) The Director agreed that DCAA does not have co-utilization agreements at all locations. She stated that DCAA has a current co-utilization agreement for the Regional Office and DoD OIG (b) (7)(E) DCAA (b) (7)(E). The Director noted, however, that in April 2016 DCAA submitted NRO (b) (3), 10 USC § 424

[REDACTED]
[REDACTED]
The Director also stated that FD does not have detailed information on security incidents. As a result, in January 2016 FD developed and implemented a standard operating procedure for reporting, tracking, and investigating FD security incidents.

The Director agreed that not all corrective actions were addressed from the May 2012 Staff Assistance Visit conducted by DoD SAPCO.

Our Response (U)

(U//~~FOUO~~) Our findings and conclusions were based on observations made and analysis conducted throughout the audit. Our finding that FD did not comply with DoD security guidance was based on multiple instances of non-compliance. For example, the Director agreed that the FD lacked co-utilization agreements and detailed information on security incidents. Before the audit began (November 5, 2015), we requested copies of DCAA's internal guidance, such as security policies and standard operating procedures to determine whether these aligned with DoD guidance. Our review of DCAA's guidance showed that it had not been updated when DoD security guidance was revised on June 18, 2015.

(U) We do not agree with the Director's position that classification reviews are not necessary when documents contain information extracted from other classified documents. Specifically, FD personnel were not following DoD Manual 5200.01, volume 1, which requires derivative classifiers to analyze the material they are classifying against the security classification guide or contact the originator of the source document if the source document is not sufficient to make a classification determination. As stated in the report, FD officials acknowledged that they did not always receive security classification guides. In addition, source documents do not always provide sufficient guidance related to the compilation of information.

(U//~~FOUO~~) Our conclusion that the FD ~~DCAA (b) (7)(E)~~ was based on the examples cited in the report. ~~DCAA (b) (7)(E)~~ is defined by DoD Manual 5205.07, volume 1, as ~~DCAA (b) (7)(E)~~

~~DoD OIG (b) (7)(E)~~ For example, as stated in this report, allowing FD staff ~~DoD OIG (b) (7)(E)~~

~~DoD OIG (b) (7)(E)~~

~~DoD OIG (b) (7)(E)~~

also constitutes ~~DCAA (b) (7)(E)~~

Management Comments on Adequacy of Protecting Classified Information (U)

(U) The Security Director, DoD SAPCO, responding for the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office stated

that in over four years of working with DCAA FD he has never received a clear answer on what SAP information is required for each type of audit FD conducts. The Security Director added that this is important in identifying who needs access to SAP programs, where they need to access SAP data, and if any SAP data is required for processing or retaining at FD facilities.

Our Response (U)

(U) We agree with the Security Director, DoD SAPCO, and made recommendations to address his concerns (see Recommendation A.3.h).

(U) Recommendations, Management Comments, and Our Response

(U) Revised Recommendation

(U) As a result of comments from the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office, we revised draft Recommendation A.1.b, to include the results of the risk assessment to satisfy Recommendation A.1.a.

(U) Recommendation A.1

(U//~~FOUO~~) We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office:

- a. (U//~~FOUO~~) Conduct a risk assessment on the all missing Defense Contract Audit Agency security incident information.

Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office Management Comments (U)

(U) The Security Director, DoD SAPCO, responding for the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office, agreed with the recommendation. The Security Director instructed the Chief of Security Oversight and Compliance Branch to conduct a risk assessment of all missing FD security incident information and provide a preliminary report within 90 days, provided DoD SAPCO receives support from DCAA to conduct the risk assessment.

Our Response (U)

(U) The Security Director, DoD SAPCO, addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we receive and review the results of the risk assessment.

- b. (U) Upon completion of Recommendation A.1.a (above), work with the Defense Contract Audit Agency Security Officer to prioritize security vulnerabilities for remediation and establish timelines for completion.**

Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office Management Comments (U)

(U//~~FOUO~~) The Security Director, DoD SAPCO, responding for the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office, agreed with the original recommendation. The Security Director stated that only

DoD OIG: (b) (7)(E)

Also, the Security Director stated that he has waited more than two years for FD to provide the requirements for SAP facilities and information technology systems and has not received any information. Therefore, the Security Director has instructed both FD and its customers to use existing customer SAP facilities and not bring SAP information into unapproved facilities. The Security Director stated that during the risk assessment DoD SAPCO will identify any information that has been brought into non-accredited facilities.

(U) Our Response

(U//~~FOUO~~) The Security Director, DoD SAPCO, partially addressed the recommendation; therefore, the recommendation is unresolved. The action initiated by the Security Director only addresses DoD OIG: (b) (7)(E)

The response does not prioritize the other security vulnerabilities, such as co-utilization agreements, security classification reviews, security incident reporting, SAP accesses, document accountability discussed in the report, or establish timelines for DCAA's completion. Therefore, we request that the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office prioritize all security vulnerabilities for remediation and establish timelines for completion. We will close the recommendation after we verify that security vulnerabilities have been prioritized for remediation and actions have been completed to correct the security vulnerabilities.

Recommendation A.2 (U)

(U) We recommend that the Director, Defense Contract Audit Agency:

- a. **(U) Review and evaluate the leadership and performance of the Regional Director of Field Detachment, and report on what if any management action has been taken.**
- b. **(U) Designate Field Detachment security duties to a qualified security official.**
- c. **(U) In coordination with the Defense Contract Audit Agency Security Officer develop and implement a formalized program access request process to initiate, approve, debrief, and maintain personnel accesses.**
- d. **(U) Authorize property accountability officials to update property accountability files.**
- e. **(U) Dispose of damaged and excess equipment.**
- f. **(U//~~FOUO~~) Initiate corrective action to the 2012 Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office Staff Assistance Visit report.**

Defense Contract Audit Agency Comments (U)

The Director, DCAA agreed, stating that: (U)

- (U) the FD Regional Director was reassigned in November 2016,
- (U) all security functions were centralized under the agency Security Officer effective January 1, 2016,
- (U) beginning February 1, 2017, DCAA implemented a formalized PAR process, including a new PAR form and standard operating procedure that will be issued by June 2017,
- (U) all FD trained and certified property custodians are now authorized to access accountability files and property systems, and all FD property custodians received property management training in May 2016,
- (U) during FY 2016 and 2017 every FD FAO had removed all damaged and excess property in accordance with DCAA Instruction 5000.17, and

- (U) In February 2017, DCAA established a team dedicated to addressing the audit and security requirements for FD. When this team completes its work in December 2017, audit and security policies and procedures will be established to ensure compliance with DoD directives, policies, and guidelines for safeguarding and protecting classified information.

(U) In addition, the Director stated that DCAA requested another face-to-face meeting with the audit team to receive clarification on the findings and that meeting never occurred.

Our Response (U)

(U//~~FOUO~~) The Director, DCAA, addressed all specifics of the recommendations; therefore, Recommendations A.2.a, A.2.b, and A.2.d are closed and A.2.c, A.2.e, and A.2.f are resolved. We will close Recommendation A.2.c when we review and verify that DCAA has developed and implemented a formalized PAR process, including a new standard operating procedure, and updated PAR form; Recommendation A.2.e, when we receive a listing of all damaged and excess property that had been turned in and destruction records; and Recommendation A.2.f, when we receive a listing of all new or revised audit and security policies issued and the corrective actions completed addressing the 2012 DoD SAPCO Staff Assistance Visit Report.

(U) In addition, we do not agree with the Director's position that a meeting on clarification of the findings never occurred. We met with the FD Regional Director and her staff on April 20, 2016, and September 20, 2016, the Director, DCAA, on April 22, 2016, and the Deputy Director, DCAA, on December 14, 2016, to provide clarification on the findings.

(U) Recommendation A.3

(U) We recommend that the Defense Contract Audit Agency Security Officer:

- (U//~~FOUO~~) Identify and complete all required co-utilization agreements for the Defense Contract Audit Agency Field Detachment.**
- (U//~~FOUO~~) Update internal guidance to require classification reviews from the customer program security officer for audit work derived from classified information.**

- c. (U//~~FOUO~~) Develop and implement an incident response plan, including updated policies and procedures, for reporting, tracking, and investigating Field Detachment security incidents.
 - 1. (U) Restrict non-security employee access to incident logs.
- d. (U) Update the SF 700s with the required information and limit access to the special access programs ^{DoD OIG: (b) (7)(E)} [REDACTED] [REDACTED] to those who are approved for access.
- e. (U) Implement the use of authorized access lists and visitor logs in Defense Contract Audit Agency Field Detachment computer server rooms.
- f. (U) Appoint its general special access program security officers in writing.
- g. (U//~~FOUO~~) Complete special access program facility accreditation documentation for the Defense Contract Audit Agency Field Detachment locations.
- h. (U//~~FOUO~~) Work with the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office to identify all Field Detachment personnel special access program accesses.
- i. (U) In coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office, develop and implement a formalized automated process to request, initiate, approve, debrief, and maintain personnel special access program accesses.
 - 1. (U) Debrief all personnel that do not have a valid need-to-know, are not clearly and materially contributing to the oversight of the special access program, and no longer require access to the information.
 - 2. (U) Develop and maintain a special access program master list, and provide site specific access lists to the Field Detachment security managers.

3. (U) Require security managers to destroy the old document when they receive an updated list.
4. (U) Inform the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office of all updates to DoD ^{DCAA: (b) (7)(E)} [REDACTED] accesses.
- j. (U) Update, complete, sign, and disseminate security policies and procedures.
- k. (U) Develop a separate automated accountability systems for Top Secret collateral and special access program material. The accountability system must be standardized and include the minimum required information found in the DoD Manual 5200.01, volume 1, "DoD Information Security Program, Overview, Classification, and Declassification," February 24, 2012.
- l. (U) Work with the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office to identify and grant access to the Top Secret Control Officers, alternate Top Secret Control Officers, and the designated disinterested persons responsible for the accountability system.
- m. (U) Require all Defense Contract Audit Agency personnel performing audits of classified and special access program contracts receive mandated training and track all training.
- n. (U//~~FOUO~~) Initiate corrective action based on the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office risk assessment.

Defense Contract Audit Agency Comments (U)

(U) The Director, DCAA, responding for the DCAA Security Officer, agreed with Recommendations A.3.a, A.3.c, A.3.c.1, A.3.d, A.3.e, A.3.f, A.3.g, A.3.h, A.3.i, A.3.i.1, A.3.i.2, A.3.i.3, A.3.j, A.3.k, A.3.l, A.3.m, and A.3.n. The Director cited a number of specific actions that had been initiated in response to these recommendations. For the full text of the Director's comments, see the Management Comments section of this report. The Director, DCAA, requested that the audit team provide clarification on the finding as it

relates to physical security and the protection of classified material currently located within a SCIF (Recommendation A.3.g).

(U) The Director partially agreed with Recommendations A.3.b and A.3.i.4. Specifically, the Director did not agree that classification reviews of documents containing information extracted from other classified documents was required. The Director stated that FD personnel are derivative classifiers and not original classifiers and the FD supervisors validate that documents are appropriately classified by using the source document, consulting with the originator of the document, or consulting with the agency security office. If a document is not appropriately portion marked, the supervisors will direct FD personnel to coordinate with the customer Program Security Office. The Director, DCAA, did not agree that FD should provide DoD SAPCO with information ^{DCAA: (b) (7)(E)} and requested further clarification from the audit team on the policy requirements for providing ^{DoD OIG: (b) (7)(E)} to the DoD SAPCO.

Our Response (U)

(U) The Director, DCAA, addressed all specifics for Recommendations A.3.a, A.3.c, A.3.c.1, A.3.d, A.3.e, A.3.f, A.3.i, A.3.i.1, A.3.i.2, A.3.i.3, A.3.j, A.3.k, A.3.l, A.3.m, and A.3.n; therefore, these recommendations are resolved. We will close the recommendations when DCAA provides:

- (U//~~FOUO~~) verification that all co-utilization agreements have been approved,
- (U//~~FOUO~~) copies of security incident standard operating procedures, security incident forms, and training certificates,
- (U//~~FOUO~~) results of the Security Office's review of Standard Form 700s,
- (U//~~FOUO~~) copies of all general SAP security officer appointment letters,
- (U//~~FOUO~~) copies of the access roster and a sample visitor log for FD computer server rooms,
- (U//~~FOUO~~) verification that the Security Information Management System will be used to maintain a log of SAP accesses,
- (U//~~FOUO~~) confirmation of total personnel debriefed from SAPs and copies of destruction certificates for outdated access rosters,

- (U//~~FOUO~~) copies of all updated security policies and procedures,
- (U//~~FOUO~~) notification that Security Information Management System has been fully deployed and is the system of record for maintaining accountability logs for Top Secret collateral and SAP materials,
- (U//~~FOUO~~) a listing of all primary and alternate Top Secret Document Control Officers and copies of rosters or training certificates completed for mandatory annual and refresher security training, and
- (U//~~FOUO~~) results of the risk assessment performed with the DoD SAPCO and corrective actions completed from that assessment.

(U//~~FOUO~~) The Director, DCAA, did not address all specifics for Recommendations A.3.b, A.3.g, A.3.h, and A.3.i.4; therefore, the recommendations are unresolved. Regarding Recommendation A.3.b, we disagree with the Director's position that classification reviews are not required and that FD supervisors are validating that documents are appropriately marked. During our site visits, FD personnel stated that instead of requesting a classification review from the customer program security officers, FD conducted the review. DoD Manuel 5200.01, volume 1, requires derivative classifiers to analyze the material they are classifying against instruction provided in a security classification guide or contact the originator of the source document if the source document is not sufficient. Relying solely on the classification of the source documents does not always take into account compilation of information. Therefore, the DCAA Security Officer should provide comments to the final report addressing actions she will take to ensure classification reviews are conducted by the respective program security office. We will close the recommendation after we review and verify that DCAA classification procedures include coordination with the appropriate program security office.

(U//~~FOUO~~) Although the Director agreed with Recommendation A.3.g, she did not address the specifics of the recommendation. The DCAA Security Officer should ensure that SAP audits are performed in SAP accredited facilities. Performing SAP audits in SAP accredited facilities will address our observations DCAA (b) (7)(E)

[REDACTED]. For example, we observed that FD branch offices were accredited DoD OIG (b) (7)(E)

[REDACTED] Therefore, we request that the DCAA Security Officer provide comments to the final report addressing actions she

has taken or will take to obtain SAP accreditation for the DCAA FD offices. We will close the recommendation after we receive and review the updated SAP facility accreditation documentation for all FD locations.

(U//~~FOUO~~) The Director partially agreed with Recommendation A.3.h. However, we do not agree that the BPIT team has identified all FD personnel SAP accesses (including DoD OIG: (b) (7)(E)). Our conclusion that the BPIT did not identify all FD accesses was based on specific examples cited in the report. For example, the Director stated that the BPIT team used the Joint Access Database Environment to identify accesses by person; however, the database does not account for the DoD OIG: (b) (7)(E) . Without knowledge of both DoD OIG: (b) (7)(E) , Therefore, the DCAA Security Officer should provide comments to the final report addressing actions she will take to identify all DCAA: (b) (7)(E) . We will close the recommendation once we verify that the Security Officer has identified the SAP accesses of all DCAA staff.

(U//~~FOUO~~) The Director, DCAA, did not address all specifics for Recommendation A.3.i.4; therefore the recommendation is unresolved. FD should provide DoD SAPCO with the unclassified program identifiers for all DoD OIG: (b) (7)(E) that reside in DoD facilities and the FD personnel briefed to those programs. As the Cognizant Authority for DCAA, the DoD SAPCO has responsibility for providing security oversight, facility accreditation, and support functions regarding DCAA SAP efforts. That information is also required for FD to obtain co-utilization agreements for FD sites. If DCAA chooses to not provide the information to the DoD SAPCO and stores information DoD OIG: (b) (7)(E) in DCAA: (b) (7)(E) , it would prevent DCAA from obtaining approval of the co-utilization agreements. Therefore, the DCAA Security Officer should provide comments to the final report addressing the procedures she will implement to inform the DoD SAPCO on a recurring basis of all DoD OIG: (b) (7)(E) for DCAA staff. We will close the recommendation when we review, and verify, that the DoD SAPCO has been informed of the DoD OIG: (b) (7)(E) of DCAA staff.

Finding B (U)

FD Did Not Effectively Use Personnel and Facilities to Support SAP Contract Audits (U)

(U) DCAA leadership did not effectively use FD personnel and facilities to support classified and SAP contract audits. This occurred because:

- (U) DCAA leadership placed a priority on non-SAP contract audits;
- (U) FD leadership did not have a process for identifying SAPs to perform audit planning and oversight of classified and SAP contracts; and
- (U) FD did not identify a classified automated information system for conducting classified and SAP audit assignments and reports.

(U//~~FOUO~~) As a result, DoD OIG: (b) (7)(E)

Management of Field Detachment Personnel and Facilities to Support Classified and SAP Audits (U)

(U//~~FOUO~~) DCAA leadership was not effectively using FD personnel and facilities to support classified and SAP contract audits. According to DoD Directive 5205.07, the FD will maintain a sufficient group of personnel who are responsible for conducting audits of SAP contracts. However, a majority of FD cleared personnel and secure facilities were not being used to support classified and SAP contract audits.²⁷

(U//~~FOUO~~) FAO branch managers, supervisors, and personnel stated that unclassified incurred cost audits and demand work makes up at least DoD OIG: (b) (7) of FDs

²⁷ (U) For the purposes of this report, FD and DCAA personnel with Top Secret and sensitive compartmented information access are called "cleared," and staff without those accesses are called "Uncleared."

assignments.²⁸ We observed cleared FD personnel only working on unclassified assignments (including unclassified disclosure statement audits, direct cost and proposal audit). In some instances FD personnel have not worked on classified or SAP assignments in over three years. In addition, we also observed that FD personnel at the branch offices and regional office are on regular telework schedules. Therefore, FD personnel cannot work on classified and SAP contract assignments while teleworking. Specifically, FD personnel we interviewed are allowed to telework from one to four days per week. DCAA needs to identify and include FD mission requirement for conducting audits of classified and SAP contracts into the annual planning process and reassess the use of regular telework schedules to ensure adequate personnel are available to audit classified and SAP contracts.

DoD OIG: (b) (7)(E)

(U)

(U//~~FOUO~~)

DoD OIG: (b) (7)(E)

(U//~~FOUO~~) As discussed in Finding A, we also identified DoD OIG: (b) (7)(E)

Requiring personnel to review the DD Form 254, "DoD Contract Security Classification," will alert the uncleared auditor that the contract involves classified information DCAA: (b) (7)(E)

.²⁹ Reviewing the DD Form 254 is also a mechanism to verify FD is aware of and conducting oversight of classified and SAP efforts in accordance with its mission and DoD guidance. DCAA must require personnel to review the DD Form 254 as part of

²⁸ (U) Demand work includes customer requested assignments; proposal audits; forward pricing rates; terminations; claims; and other time-sensitive requests.

²⁹ (U) The DoD Form 254 identifies the level of classification the contractor will require in performing the contract.

the audit program plan before performing a review, and notify FD if the effort is classified.

FD Facility Usage (U)

(U//~~FOUO~~) We identified SCIFs maintained by FAOs that were unoccupied at the same time cleared personnel were permanently working in unclassified facilities (known as “tank space”). For example, the DoD OIG: (b) (7)(E) branch manager decided to permanently locate cleared staff in an unclassified facility because the staff did not always work on classified or SAP audits. According to the branch manager, the unoccupied SCIFs are used when a cleared person needed to work on classified information. We reviewed the SF700s and determined that the SCIF spaces were rarely opened and cleared personnel only entered the SCIFs to log into their global wide area network accounts to keep the accounts active. As result, FD SCIFs are not being used for their intended purpose and FD personnel cleared to Top Secret//Sensitive Compartmented Information are working primarily in unclassified facilities, on unclassified projects.

(U//~~FOUO~~) As part of its duties, the BPIT identified DoD OIG: (b) (7)(E) SCIFs to close. We commend the BPIT for the proactive steps taken in this instance. However, the process the BPIT used to identify unused SCIFs was not based on established criteria, such as workload or cleared personnel. Therefore, FD should conduct an assessment of all FD facilities based on specific criteria to determine whether the facilities are being used for their intended purpose.

Non-SAP Audit Priorities (U)

(U//~~FOUO~~) DCAA leadership was not effectively using FD personnel and facilities to support classified and SAP contract audits because DCAA leadership placed a priority on conducting non-SAP contract audits. For example, the DCAA FY 2015 and FY 2016 annual planning guidance set the DCAA’s focus on reducing the backlog of incurred cost audits because those audits require the greatest amount of resources. The planning guidance stated that incurred cost audits are the DCAA’s highest overall priority workload. The planning guidance did not identify FD classified and SAP audit efforts.

FD Oversight (U)

(U//~~FOUO~~) FD leadership did not have a process for identifying SAPs. Specifically, FD leadership did not coordinate and plan for performing and overseeing audits of classified and SAP contracts.

Coordination and Planning of Classified Contracts (U)

(U//~~FOUO~~) FD leadership did not adequately coordinate and plan for identifying and performing oversight of classified and SAP contracts. FD identifies SAP contracts when a customer requests audit services, such as signing vouchers. Without notification from the customer, FD is not aware that the classified and SAP efforts exist. However, FD should not rely on voucher reviews or customer notification because FD personnel are aware of customers who have not been forthcoming. For example, FD personnel are aware of customer vouchers that are reviewed directly by the contracting officer and not reviewed and processed by FD. DoD OIG: (b) (7) Branch Office personnel are aware of a large SAP contract that was not part of the DCAA annual plan.

(U//~~FOUO~~) In addition, FD personnel have also identified SAPs during mandatory annual audit requirement [MAAR] 6 reviews that are not part of the DCAA annual plan. The FD Regional Director stated that she cannot guarantee that FD had identified all classified and SAP contracts. Instead, FD leadership relies on the customer to notify and identify classified and SAP contracts to conduct oversight. FD cannot perform audit oversight of potentially high risk contracts without knowledge of all SAP contracts. FD needs to establish a process with customers for coordinating and planning all classified and SAP efforts on at least an annual basis or more often if needed. This information should be used by FD leadership to plan audit oversight efforts for classified and SAP projects.

Access to SAP Programs (U)

(U//~~FOUO~~) FD leadership and branch managers did not request access to the SAPs for which they are responsible for conducting audit planning and oversight. The FD Regional Director stated that she and FD leadership did not have the SAP accesses necessary to identify SAP efforts. However, it is FD leadership's responsibility to coordinate with the customers, identify the SAP, and contact the DoD SAPCO for access. Therefore, without access, FD cannot conduct classified discussions and review customer data to conduct audit planning and oversight. In addition, FD is not providing

adequate supervision and oversight of SAP audit assignments in accordance with Government Auditing Standards.³⁰ Government Auditing Standards state that supervisors must review the audit work performed. We determined that at the DoD [redacted] Branch office and other FAOs only one person was briefed and working on a SAP and the direct supervisor or the branch manager did not have access to the SAP to provide supervision and oversight. FD needs a designate a group of FD leadership and branch managers and coordinate with DoD SAPCO, to receive access to SAPs to conduct planning and oversight of SAPs.

Classified Automated Information System (U)

(U//~~FOUO~~) FD did not maintain a classified automated information system for conducting classified audit assignments and reports.

DoD OIG: (b) (7)(E)

(U)

(U//~~FOUO~~) FD used DoD [redacted] until 2014 to conduct work on all unclassified, classified, and SAP audits. In August 2014, officials at the National Reconnaissance Office, the system authorizer, found that DoD [redacted] no longer complied with the terms and conditions of its system authorization. Specifically, DoD OIG: [redacted] was only authorized to process sensitive compartmented information in the National Reconnaissance Office. However, FD was processing unclassified, classified, and SAP information from multiple customers on DoD OIG: [redacted]. Accordingly, the National Reconnaissance Office terminated DoD OIG: [redacted]. As of January 2017 FD leadership had not identified a replacement classified automated information system for conducting classified audit assignments and reports. As a result, FAOs have reduced the number of classified audit reports and have withdrawn requests for classified assignments.

(U//~~FOUO~~) The FAOs have reduced the number of classified audit reports issued since the termination of DoD OIG: [redacted]. According to FD supervisors, they have withdrawn requests for classified assignments because the lack of a classified automated information system would require that the work be done manually and maintained in hardcopy format. In addition, FD personnel attributed the reduction in the number of classified documents the FAOs received to the lack of a classified automated capability. When DoD [redacted] was operational, FD personnel could receive classified data electronically. However, FD personnel must now print all classified documents from the customer and contractor

³⁰ (U) GAO-12-331G, "Government Auditing Standards", 2011 Revision, section 6.54.

facilities. FD personnel stated that printing documents increased audit wait times and they do not have the space to store the documents. Consequently, FD personnel are

DoD OIG: (b) (7)(E)

Security of Audit Data (U)

(U//~~FOUO~~) According to FD personnel,

DoD OIG: (b) (7)(E)

Conclusion (U)

(U//~~FOUO~~) FD has responsibility for the overall planning, management, and execution of DCAA contract audits of classified programs and SAPs. FD is not effectively using cleared FD personnel and facilities to audit classified system and SAP contracts. FD cannot provide adequate oversight of contractor financial and accounting records which leaves DoD vulnerable to inaccuracies in financial statements and reporting. As a result,

DoD OIG: (b) (7)(E)

Management Comments on the Finding and Our Audit Response (U)

Management Comments on the Use of FD Personnel and Facilities to Support Classified and SAP Contract Audits (U)

(U//~~FOUO~~) The Director, DCAA, did not agree with the finding, stating that the report did not identify any security or audit concerns that substantiate the finding. The Director also did not agree that DCAA leadership did not effectively use FD personnel and facilities to support classified and SAP contract audits. The Director stated that

DCAA leadership does not place priority on non-SAP contract audits and that all contractor work must be audited to provide the necessary audit advice on classified contracts. She also stated that classified contracts are prioritized the same as non-classified contracts. The Director stated that the DCAA's planning guidance does not separately identify classified work as a top priority; rather the DCAA's top priorities are applied to FD's audit work. In addition she stated that the DCAA leadership does have a process for identifying SAPs and cited Federal Acquisition Regulation (FAR) Part 4, "Administrative Matters," Subpart 4.2, "Contract Distribution," which requires contracting officers to notify DCAA of contract awards. Other methods of identifying SAP work cited by the Director included notification by the contractor, Financial Liaison Advisors, submission of contractor vouchers, contractor incurred cost proposals, customer meetings, mandatory annual audit requirements [MAAR], and the annual SAP report to Congress.

(U//~~FOUO~~) The Director stated that the system FD used to conduct classified audits was shut down in August 2014, at the direction of the National Reconnaissance Office. According to the Director, FD currently relies on DoD OIG: (b) (7)(E) approved classified systems and was in the process of obtaining access to additional systems at all appropriate locations. The Director did not agree that a majority of FD cleared personnel and security facilities were not being used to support classified and SAP contract audits. She noted that all contractor work must be audited to provide the necessary audit advice on a classified contract and that it may be more efficient for a cleared auditor to perform the complete audit based on the type of audit and the steps required. The Director did not agree that FD is not providing adequate supervision and oversight of SAP audit assignments in accordance with Government Auditing Standards. The Director stated that there are cases where an employee's immediate supervisor or branch manager does not have access to the SAP to provide supervision and oversight due to several factors such as limited available security billets, sensitivity of programs, or audit efficiency. However, in those cases, the Director stated the audit work was supervised by a different person who has the proper accesses. According to the Director, if supervisors do not have the proper accesses for adequate supervision, the supervisor disengages.

Our Response (U)

(U//~~FOUO~~) Our findings and conclusions were based on observations made and analysis conducted throughout the audit. During our site visits we were repeatedly

informed by FD personnel that the DACC's highest priority was unclassified incurred cost audits. In addition, the DCAA FY 2015 and 2016 annual planning guidance focused on reducing the backlog of incurred cost audits because those audits require the greatest amount of resources. In addition FAR Part 4 only requires DCAA be notified of contract distribution, not whether the contract contains any classified or SAP elements. Although it is important to reduce backlogs of audits, doing so should not increase the risk of not conducting audits of the DoD's sensitive programs.

(U//~~FOUO~~) Our finding that FD did not identify a classified automated information system for conducting classified and SAP audit assignments was based on documentation and discussions with the FD Regional Director. As of May 2017, FD leadership still had not identified a replacement system for conducting classified audit assignments and reports since the August 2012 termination of DoD OIG: (b) (7)(F). In addition, FD personnel notified us that they were DoD OIG: (b) (7)(E)

(U//~~FOUO~~) We disagree that FD is providing adequate supervision. For example, we note in the report an instance where only one auditor in FD had access to a SAP. The auditor's supervisor or branch manager or another supervisor did not have access for any of the reasons the Director cited (limited available security billets, sensitivity of programs, or audit efficiency). It is not clear how the audit is being adequately supervised in accordance with generally accepted government auditing standards.

Recommendations (U)

Recommendation B.1 (U)

(U) We recommend that the Director, Defense Contract Audit Agency:

- a. (U) Ensure special access program contract audits are included in Defense Contract Audit Agency annual planning guidance.

(U) Defense Contract Audit Agency Comments

(U) The Director, DCAA, agreed stating that the DCAA's yearly staff allocation and future plan guidance addresses all of its unclassified and classified workload. DCAA's guidance

does not separately identify classified work as a top planning priority. Rather, it identifies types of audits that are prioritized, which FD uses to plan the audits for contractors under its cognizance and to coordinate completion of the direct cost audits of classified and SAP contracts with the cognizant Regional FAO. The Director stated that it was not in DCAA's control to know all of the classified contracts issued. She stated that it is the Contracting Officer's responsibility to notify DCAA when a classified contract is issued; however, FD personnel have many processes to identify SAP work.

Our Response (U)

(U) The Director, DCAA, did not address all specifics of the recommendation; therefore, the recommendation is unresolved. According to the DCAA audit plan the highest priority is placed on conducting non-SAP contract audits. The DCAA FY 2015 and FY 2016 annual planning guidance set DCAA's focus on reducing the backlog of incurred cost audits because those audits required the greatest amount of resources. This was reflected in the type of audit work FD personnel predominately conducted. In addition, during our site visits we were repeatedly informed by FD personnel that the agency's highest priority and workload was incurred cost audits. This included audits that were not part of FD's normal work load. FD needs to focus on classified and SAP work in accordance with DoD Directive 5205.07. Therefore, the Director should provide comments to the final report describing the percentage of FD's classified and SAP workload and how DCAA plans to meet the intent of the DoD Directive 5205.07. We will close the recommendation after we verify that DCAA fully addressed the recommendation.

- b. (U) Notify all DCAA employees that the Field Detachment is responsible for performing all audit assignments involving classified and special access program contracts.**

Defense Contract Audit Agency Comments (U)

(U//~~FOUO~~) The Director, DCAA, disagreed stating that the report implies that cleared people must perform all audits that may impact classified and SAP contracts. She stated FD is responsible for performing the parts of the audit assignment involving access to classified information. Also, uncleared auditors are aware that FD is the organization that must be contacted if clearances are required to appropriately complete an audit step or perform an audit. The Director stated that FD leadership will brief all DCAA

management on FD's mission and responsibilities in the June and July 2017 Agency supervisory workshops.

Our Response (U)

(U//~~FOUO~~) The Director, DCAA, did not address all specifics of the recommendation; therefore, the recommendation is unresolved. We disagree that DCAA personnel are aware that the FD is responsible for performing classified and SAP audits. For example, FD staff told us that DoD OIG: (b) (7)(E)

[REDACTED] It is critical that FD staff also perform audits that impact classified contracts. DCAA (b) (7)(E)

[REDACTED]. Therefore, the Director should provide comments to the final report and describe what actions will be taken to DoD OIG: (b) (7)(E)

[REDACTED]. We will close the recommendation after we review, and verify, procedures implemented by DCAA to notify staff of the mission and responsibilities of FD and verify that cleared FD staff are performing audits that impact classified contracts.

- c. **(U) Establish an agency wide process requiring auditors to review the DD Form 254, "DoD Contract Security Classification Specification," as part of the program audit plan before performing a review of the contract.**

Defense Contract Audit Agency Comments (U)

(U) The Director, DCAA, partially agreed. The Director did not agree that the existence of a DD Form 254 automatically means a cleared auditor is required to perform the audit. The Director agreed that the DD Form 254 indicates potential contracts that require further review by cleared personnel, but that all auditors are aware that FD is the organization that will perform audit work that requires clearances and that this would be a topic during DCAA 's supervisory workshops.

Our Response (U)

(U//~~FOUO~~) The Director, DCAA, did not address all specifics of the recommendation; therefore, the recommendation is unresolved. We agree that the existence of a DD 254

does not by itself mean a cleared auditor is required to perform the audit. However, reviewing the DD 254 as part of the audit plan will alert the uncleared auditor that the contract involves classified information ^{DCAA (b) (7)(E)} [REDACTED]

[REDACTED] The Director, DCAA should provide comments to the final report addressing actions she will take to require auditors to review the DD Form 254 for potential classified or SAP contracts. We will close the recommendation after we review and verify the procedures implemented to notify auditors of the need to review DD Form 254s for potential classified audit work.

- d. **(U) Based on the results of recommendation B.1.c (above) notify the Field Detachment of all classified, sensitive compartmented information, and special access program related efforts.**

Defense Contract Audit Agency Comments (U)

(U) The Director, DCAA, agreed, stating that DCAA will prepare training for all supervisory auditors on what to do when classified contracts are identified during an audit. This training will be given during a supervisory auditor workshop in June and July 2017.

Our Response (U)

(U) The Director, DCAA, addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we review and verify that the training addresses the requirement to notify FD of all classified and SAP efforts and verify that the training was completed.

(U) Recommendation B.2

(U) We recommend that the Field Detachment Regional Director for Defense Contract Audit Agency:

- a. **(U) Perform an annual assessment of Field Detachment staffing and facility requirements for audit oversight of classified and special access programs operations based on established criteria.**
 1. **(U) The criteria must include the volume of classified and special access programs workload at each site; the number of cleared personnel; and future audit requirements.**

2. **(U) The group should include involvement from Defense Contract Audit Agency Security Division and staff of equivalent responsibilities and authority.**
3. **(U) Identify and grant access to those Field Detachment employees designated to perform audits of classified and special access programs.**

(U) Defense Contract Audit Agency Comments

(U) The Director, DCAA, responding for the FD Regional Director, agreed, stating that FD has always performed an annual assessment of staffing and facility requirements to adequately perform its mission. The Director added that FD recently established a program access response team, which includes the Agency Security Division, to address future facility requirements and sensitive compartmented information/SAP needs for auditors. The team is expected to complete its review by December 2017.

(U) Our Response

(U) The Director, DCAA, addressed all specifics of the recommendations; therefore, the recommendations are resolved. We will close Recommendation B.2.a, B.2.a.1, B.2.a.2, and B.2.a.3, when we receive the results of the program access review team and verify that the FD facility requirements meet the sensitive/SAP needs of the audit staff.

- b. **(U) Establish and implement a process for annual planning and coordination with customer program security officers and Field Detachment supervisors to identify classified and special access programs.**

(U) Defense Contract Audit Agency Comments

(U) The Director, DCAA, responding for the FD Regional Director, partially agreed, stating that it was part of FDs planning process to identify and audit contractor processes and claimed costs impacting classified contracts. FD has a process for identifying SAP contracts, employing many techniques to identify classified workload. The Director stated that having to coordinate with every customer program security officer would place an undue burden on DCAA since it supports hundreds of programs. According to the Director, FD leadership has placed emphasis on meeting the customers' needs in many ways. For example, FD has established six customer-centric

audit teams to address the audit needs of the command expediently. FD leadership has assigned Financial Liaison Advisors at many of the commands with classified work. Those Advisors expedite the communication and planning between the program office and the auditors. The Director added that DCAA will coordinate with the DoD SAPCO to explore the possibility of coordinating with individual SAPCOs of major DoD components to assist in identifying contracts. However, she stated that ultimately it is the contracting officer's responsibility to notify DCAA of contract awards as stated in the Federal Acquisition Regulation.

Our Response (U)

(U) Although the Director, DCAA, only partially agreed, the comments addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation when we review and verify the results of DCAA's coordination with the DoD SAPCO regarding identifying classified and SAP contracts with the individual SAP security offices.

1. **(U) Work with Defense Contract Audit Agency Security Officer and the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office, to designate a group of Field Detachment leadership and branch managers, to receive access to special access programs to conduct planning and oversight.**

Defense Contract Audit Agency Comments (U)

(U//~~FOUO~~) The Director, DCAA, responding for the FD Regional Director, disagreed, stating that designating a group of FD and branch managers to receive access to SAPs to conduct planning and oversight is contrary to direction of the DoD SAPCO and the National Reconnaissance Office, Director, Office of Security and Counterintelligence, to limit accesses and secure facilities.

Our Response (U)

(U//~~FOUO~~) Comments from the Director did not address all specifics of the recommendation; therefore, the recommendation is unresolved. DCAA leadership cannot adequately plan for oversight if it does not have access to the SAPs. We are not recommending that all FD personnel be provided access to SAPs to conduct planning; however, the FD leadership team, the Director, DCAA, and Deputy Director, DCAA

should have access to facilitate adequate planning. Designating a group to receive access is not contrary to direction received from the DoD SAPCO. Therefore, the FD Regional Director should provide comments to the final report addressing what actions will be taken to designate a select group to receive access to SAPs to conduct planning and oversight. We will close the recommendation after we verify that designated individuals have received accesses to SAPs for the purposes of planning and oversight.

2. (U) Conduct annual planning to identify Field Detachment audit oversight efforts for classified and special access program projects.

Defense Contract Audit Agency Comments (U)

(U) The Director, DCAA, responding for the FD Regional Director, partially agreed, stating that the comments provided to Recommendation B.2.b., in which she stated that the DCAA will coordinate with the DoD SAPCO to explore the possibility of coordinating with individual SAP security offices of major DoD components to assist in identifying contracts, applicable to this recommendation.

Our Response (U)

(U) Although the Director, DCAA, only partially agreed, her comments addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation when we receive and verify the results of DCAA's coordination with the DoD SAPCO regarding the identification of classified and SAP contracts with the individual SAP security offices.

3. (U) Reassess the use of regular telework schedules to ensure adequate personnel are available to audit classified and SAP contracts.

Defense Contract Audit Agency Comments (U)

(U//~~FOUO~~) The Director, DCAA, responding for the FD Regional Director, did not agree. The Director stated that she believes the recommendation stems from the audit team's belief that all audit effort performed at a contractor with a classified contract means that it is classified. Unclassified audit efforts exist even though the contract may have some classified parts. The Director stated that DCAA employees are eligible to telework when their positions have some duties considered portable that can be performed at

the alternate location and their performance and conduct meet the criteria required by the DoD and DCAA instructions. In determining portable work, the Director stated that the auditor and supervisor must consider the classification of the information required. For example, information obtained from a contractor's accounting system is often unclassified which allows the auditor to perform analysis, sampling, and testing at alternate locations.

Our Response (U)

(U) The Director did not address all specifics of the recommendation; therefore, the recommendation is unresolved. We are recommending that the use of telework be reassessed, not eliminated, based on the results of Recommendation B.2.b. The telework schedules for the FD staff should be based on the amount of classified and SAP audit work. The FD Regional Director should provide comments to the final report describing what actions will be taken to adjust telework schedules of FD staff based on the determination of the classified and SAP workload. We will close the recommendation after we review, and verify, the FD Regional Director's adjusted regular telework schedules for FD staff based on the amount of classified and SAP workload.

4. **(U) Determine annually whether classified, sensitive compartmented information and special access programs are receiving adequate audit oversight.**

Defense Contract Audit Agency Comments (U)

(U) The Director, DCAA, responding for the FD Regional Director, agreed and referred to the comments provided in Recommendation B.2.b, she stated that it is part of DCAA's planning process to identify and audit contractor processes and claimed cost impacting classified contracts.

Our Response (U)

(U) The Director, DCAA, addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation when we review and verify the results of DCAA's coordination with the DoD SAPCO and individual SAPCOs to identify classified and SAP contracts.

- c. (U) Acquire and use a classified automated information system for conducting classified audit assignments and reports.

Defense Contract Audit Agency Comments (U)

(U//~~FOUO~~) The Director, DCAA, responding for the FD Regional Director, did not agree, stating that DCAA needs to perform a cost benefit assessment of the feasibility of this recommendation. The Director stated that DCAA will work with the DoD SAPCO to perform this assessment. According to the Director, the report indicates that FD personnel are creating audit working papers on a contractor's system, which is not correct. The Director stated that DCAA does, in some cases, have direct access to DoD OIG: (b) (7)(E). However, she stated that the information is read only DoD OIG: (b) (7)(E). She added that currently, FAOs are using DoD OIG: (b) (7)(E). The Director stated that DCAA does not believe that utilizing DoD OIG: (b) (7)(E).

Our Response (U)

(U//~~FOUO~~) The Director, DCAA, did not address all specifics of the recommendation; therefore, the recommendation is unresolved. We disagree with the Director's comments. Once DCAA's use of DoD OIG: (b) (7)(E) was terminated, DCAA relied DoD OIG: (b) (7)(E). The SAP audit work has required not only read-only capability, but also the ability to perform analyses and create audit working papers. Until DCAA obtains its own dedicated system for performing classified and SAP audits, DoD OIG: (b) (7)(E). The Director, DCAA, should provide comments to the final report describing what actions will be taken DoD OIG: (b) (7)(E). We will close the recommendation after we review and verify the plan for acquiring the system.

Appendix A (U)

Scope and Methodology (U)

(U) We conducted this audit from September 2015 through March 2017 in accordance with General Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) We performed site visits and interviewed personnel at the following locations:

- (U) The Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office, Arlington, Virginia
- (U) DCAA, Fort Belvoir, Virginia,
- (U) FD Regional Office, DoD OIG: (b) (7)(E), Virginia,
- (U) National Reconnaissance Office, Chantilly, Virginia,
- (U) NRO: (b) (3), 10 USC § 424
- (U) FD DoD OIG: (b) (7)(E) Branch Office, NRO: (b) (3), 10 USC § 424
- (U) FD DoD OIG: (b) (7)(E) Branch Office, NRO: (b) (3), 10 USC § 424
- (U) FD DoD OIG: (b) (7)(E) Branch Office, NRO: (b) (3), 10 USC § 424
- (U) FD DoD OIG: (b) (7)(E) Branch Sub-Office, NRO: (b) (3), 10 USC § 424
- (U) FD DoD OIG: (b) (7)(E) Branch Sub-Office, NRO: (b) (3), 10 USC § 424 and
- (U) FD DoD OIG: (b) (7)(E) Sub-Office, NRO: (b) (3), 10 USC § 424

(U) We reviewed applicable guidance, including Federal regulations, and DoD directives, and instructions. We selected a non-statistical sample of DCA A- (b) employees at the FD Regional, NRO: (b) (3), 10 USC § 424, DoD OIG: (b) (7)(E) and DoD OIG: (b) (7)(E) Branch Offices and

(U) reviewed their SAP training records. We conducted a non-statistical sample of the safes, document tracking logs, and property inventory listing to review the property and document accountability at the the ^{NRO: (b) (3), 10 USC § 474} ^{DoD OIG: (b) (7)(E)} ^{DoD OIG: (b) (7)(E)} and ^{DoD OIG: (b) (7)(E)} Branch offices. We also reviewed DCAA FD security standard operating procedures and PAR records. The documentation was dated from June 1993 to December 2015.

Use of Computer-Processed Data (U)

(U) We did not use computer-processed data to perform this audit.

Prior Coverage (U)

(U) No prior coverage has been conducted on FD during the last 5 years.

(U) Management Comments

(U) DoD Special Access Program Central Office



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

OFFICE OF THE SECRETARY OF DEFENSE
3200 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

Apr 7, 2017

MEMORANDUM FOR OFFICE OF DEPUTY DEFENSE INSPECTOR GENERAL FOR INTELLIGENCE AND SPECIAL PROGRAMS ASSESSMENTS

SUBJECT: Response to Draft Report for the Audit of the Defense Audit Agency Field Detachment (Project No. D2015-DISPA3-0248,000) (U)

(U) I appreciate the work that went into completing this report. In over four years of working with DCAA I have never received a clear answer on what SAP information is required for each type of audit that DCAA/FD conducts. This is important in identifying who needs access; where do they need to access the SAP data, and if any SAP data is required for processing or retention in DCAA facilities.

(U//~~FOUO~~) Recommendation A.1.a. I agree with the recommendation and I will instruct the Chief of Security Oversight and Compliance Branch and his team to conduct a risk assessment on all the DoD OIG: (b) (7)(E) and provide a preliminary report within 90 days provided we get support from DCAA to conduct the risk assessment.

(U//~~FOUO~~) Recommendation A.1.b. DoD OIG: (b) (7)(E) DCAA facility is currently approved for SAP storage and they have no means to process SAP information in that facility or any facility for over three years. For over two years we have waited for DCAA/FD to provide the requirements for SAP facilities and IT and to date have not received any information. This is troubling given the fact that we provided over 4 full time equivalent (FTE) man years' worth of security manpower support to DCAA/FD from 2012- 2015.

(U//~~FOUO~~) DCAA: (b) (7)(E)

(U//~~FOUO~~) My action officer for support to your office on this effort is my Chief of Security Oversight and Compliance Branch, [redacted] who may be contacted at [redacted] or [redacted].

DoD OIG: (b) (6)

DoD Special Access Program Central Office

DoD OIG: (b) (6)

** REDACTED BY DoD OIG: (b) (6)
DoD SAPCO, 6-12-2017

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Management Comments

(U) Defense Contract Audit Agency



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

April 10, 2017

MEMORANDUM FOR PROGRAM DIRECTOR, READINESS AND CYBER OPERATIONS,
OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF
DEFENSE

ATTENTION: Mr. [REDACTED]

SUBJECT: DoDIG Proposed Report, Audit of the Defense Contract Audit Agency,
Field Detachment, Project No. D2015-DISPA3-0248.000, dated March 2, 2017

Thank you for the opportunity to provide comments to the subject proposed report. DCAA acknowledges areas that need improvement and have developed a corrective action plan to address the noncompliances. Overall, however, none of the noncompliances [REDACTED] DCAA: (b) (7)(E)

Enclosed is our comprehensive response to the subject report. Our response contains two enclosures. Enclosure 1 is our response to the Findings identified in the report. On October 7, 2016, we provided your office with a comprehensive response that addressed several factual discrepancies in your discussion draft report. It does not appear that our response was fully considered in this proposed report. I believe several of the findings that we disagree with stem from a misunderstanding of the Field Detachment audit operations. Once you have reviewed the DCAA response, we would like an additional meeting with the DoDIG to further explain the DCAA operations and our audit coverage of classified contracts.

Enclosure 2 is our response to the Recommendations identified in the report. We are providing a response to all the Recommendations that apply to DCAA.

If you have any additional questions or concerns, please address them to me at [REDACTED]. Thank you for your cooperation.

Anita F. Bales
Director

- Enclosures: 2
1. Response to the Findings
 2. Response to the Recommendations

ENCLOSURES 1 (5 PAGES) AND ENCLOSURE 2 (12 PAGES) WERE REDACTED BY [REDACTED] DoD OIG: (b) (6), DOD SAP CENTRAL OFFICE FROM [REDACTED] DoD OIG: (b) (6) TO THE APPROPRIATE HANDLING CAVEAT "FOUO"

DoD OIG: (b) (6)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED// [REDACTED]

● IG Draft Report-Project No. D2015-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017

(U//~~FOUO~~)

(U// [REDACTED]) FD did not comply with DoD directives, policies, and guidelines for safeguarding and protecting classified information. Report, page i, Findings:

(U) DCAA Comment: DCAA does not agree with this finding. The DoD IG implied that we do not follow any DoD directives, policies and guidelines for safeguarding and protecting classified information. FD has policies and procedures that incorporate the various DoD directives, policies, and guidelines. These have always been available for your review upon request. We believe some modifications to the wording would resolve our concerns with this finding. Based on your audit we are now aware of some areas where improvement is required.

- (U// [REDACTED]) DoD IG Finding: FD officials did not have co-utilization agreements for all locations, perform classification reviews of documents containing information extracted from other classified documents, and have detailed records of security incidents.

- (U) DCAA Comment: Co-utilization Agreements

- o (U) DCAA agrees with this finding that we do not have co-utilization agreements at all locations. As stated in our response to discussion draft, FD has a current co-utilization agreement for the Regional Office DCAA: (b) (7)(E) [REDACTED]

This co-utilization agreement covers DoD OIG: Branch Office DoD OIG: DoD OIG: (b) (7) Office DoD OIG: DoD OIG: Branch Office DoD OIG: DoD OIG: (b) Branch Office DoD OIG: NRO: [REDACTED], and DoD OIG: (b) (7)(E) Branch Office DoD OIG: in addition to the regional office.

- o (U//~~FOUO~~) In April 2016, at the request of the AT&L SAPCO the DCAA Security Office (CS) NRO: (b) (3), 10 USC § 424 [REDACTED]

- (U) DCAA Comment: Classification Reviews

- o (U) DCAA does not agree that classification reviews of documents containing information extracted from other classified document is required. As stated in our response to the discussion

Enclosure 1
(Response to Findings)
Page 1 of 5

UNCLASSIFIED// [REDACTED]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

OIG Draft Report- Project No. D2015-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017

draft, FD auditors are not original classifiers, we are derivative classifiers. Since DCAA is not the Originator, we do not have a FD Security Classification Guide. The DoD Manual 5200.01, Volume 1 dated February 24, 2012 states:

When incorporating, paraphrasing, restating, or generating classified information in a new form or document (i.e., derivatively classified information) within the Department of Defense all cleared personnel, who generate or create material that is to be derivatively classified, shall ensure that the derivative classification is accomplished in accordance with this enclosure. No specific, individual delegation of authority is required. DoD officials who sign or approve derivatively classified documents have principal responsibility of the quality of the derivative classified.

- o (U) As derivative classifiers, we follow DoD 5200.01 Volume 1 under Procedures for Derivative Classification that states:

a. Derivative Classifiers shall carefully analyze the material they are classifying to determine what information it contains or reveals and shall evaluate the information against the instruction provided by the classification guidance or the marking on source documents . . .

e. If extracting information from a document or section of a document classified by compilation, the derivative classifier shall consult the explanation on the source document to determine the appropriate classification. If that does not provide sufficient guidance, the derivative classifier shall contact the originator of the source document for assistance.

- (U) **DCAA Comment:** Security Incidents:

- o (U) DCAA agrees with this finding. Prior to August 2014, the security incident log was maintained on the ~~FD DoD OIG: (b) (7)(E)~~ is no longer being utilized; therefore, that data is unavailable. Between August 2014 and January 2016 FD maintained an informal incident log on the Regional shared drive.
- o (U) In January 2016, the CS implemented a new process and a

Enclosure 1
(Response to Findings)
Page 2 of 5

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED// [REDACTED]

OIG Draft Report- Project No. D2015-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017

standard operating procedure (SOP) has been developed and implemented for reporting, tracking, and investigating DCAA security incidents. Only the Security office has access to the security incident database. Copies of the SOPs and the security incident form are available upon request. Notification has been forwarded to the affected employees. Additional training will be provided on April 27, 2017 to all FAO Security Control Officers (SCOs).

(U//~~FOUO~~)

- (U// [REDACTED]) DoD IG Finding: FD officials [REDACTED] DoD OIG: (b) (7)(E)

(U) DCAA Comment: Accountability:

(U) DCAA does not agree with this finding. Although SAP and Top Secret information was not accounted for separately, DCAA has always performed an annual inventory of all classified materials. The inventory documentation was maintained on [REDACTED] until August 2014. Since then we are using a manual process to track and control classified materials. The CS is in the process of updating the policies and procedures for document accountability which includes utilizing an automated system that will be centrally maintained by Security.

(U//~~FOUO~~)

- (U// [REDACTED]) DoD IG Finding: FD lacked adequate policies and procedures and did not take adequate corrective actions to address the finding in the May 2012 Staff Assistance Visit conducted by the Under Secretary of Defense for Acquisition Technology, and Logistics Special Access Program Central Office. [REDACTED] DoD OIG: (b) (7)(E)
(Report, page 4, Findings)

(U) DCAA Comment: DCAA does not agree with the DoD IG conclusion that FD [REDACTED] DoD OIG: (b) (7)(E) The DoD IG provided no evidence, no recommendation and no examples in their report that FD had [REDACTED] DoD OIG: (b) (7)(E)

(U) DCAA does agree that not all corrective actions were address in the 2012 SAV report. In response, the SAPCO provided assistance by detailing two Program Security Officers (PSOs) to DCAA to assist in implementing corrective actions. Actions were taken to identify the corrections necessary and in 2015 FD established the BPIT team to address several remaining security issues not previously resolved.

Enclosure 1
(Response to Findings)
Page 3 of 5

UNCLASSIFIED// [REDACTED]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)UNCLASSIFIED// ~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED// [REDACTED]

OIG Draft Report- Project No. D2015-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment." March 2, 2017

In February 2017, the FD Deputy Regional Director established a team dedicated to address audit and security requirements for the Field Detachment. At the end of this team's assessment, audit and security policies and procedures will be established to ensure compliance with DoD directives, policies, and guidelines for safeguarding and protecting classified information. In our opinion, once completed all the SAV issues should be resolved.

(U) While DCAA agrees that we have not taken corrective actions to address all the findings in the SAV, the BPIT team addressed several of the recommendations and the current program access response team is addressing the remaining recommendations.

(U)

(U) [REDACTED] DoD IG Finding: DCAA leadership did not effectively use FD personnel and facilities to support classified and SAP contract audits. (Report, page i, Findings)

(U) DCAA Comment: DCAA does not agree with this finding. We attempted to explain to the DoD IG DCAA's mission and operations and provided a detailed rebuttal to the discussion draft. We request discussions with the DoD IG to have an opportunity to further explain DCAA's operations. As stated in our response to the discussion draft:

- (U) DCAA leadership does not place priority on non-SAP contract audits. As explained previously, all work at the contractor must be audited to provide the necessary audit advice on classified contracts. Classified contracts are prioritized the same as non-classified contracts.

(U) The Agency's planning guidance does not separately identify classified work as a top planning priority; rather the Agency's top priorities are applied to FD's audit work.

- (U) DCAA leadership does have a process for identifying SAPs. FAR Chapter 4.2 requires contracting officers to notify DCAA of contract awards. In addition, FD employs other methods to identify SAP work such as:
 - Notification by contractors;
 - FLAs;
 - Submission of contractor vouchers;
 - Contractor incurred cost proposals (Sch II);
 - Customer meetings;

Enclosure 1
(Response to Findings)
Page 4 of 5

UNCLASSIFIED// [REDACTED]

UNCLASSIFIED// ~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

OIG Draft Report- Project No. D2015-01SPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment." March 2, 2017

- Mandatory Annual Audit Requirements (MAARs); and
- Annual SAP report to Congress.
- (U//~~FOUO~~) Prior to August 2014, FD had DoD [redacted] to conduct classified audits. Upon direction of the NRO, the system was shut down in August 2014. Currently FD relies on DoD OIG: [redacted] classified systems and is in the process of obtaining access to additional systems at all appropriate locations.
- (U) DCAA does not agree with the statement supporting the finding that, "a majority of FD cleared personnel and security facilities were not being used to support classified and SAP contract audits." All work at the contractor must be audited to provide the necessary audit advice on a classified contract. This work may include audits of unclassified elements (ex. indirect costs) and audits classified in nature (ex. direct consultants). Management may determine that it is more efficient for a cleared auditor to perform the complete audit based on the type of audit and the steps required.
- (U) DCAA does not agree with the statement supporting the finding that, "FD is not providing adequate supervision and oversight of SAP audit assignments in accordance with Government Auditing Standards." There are cases where an employee's immediate supervisor or branch manager did not have access to the SAP to provide supervision and oversight due to several factors such as limited available security billets, sensitivity of certain programs, and/or audit efficiency. However, in these cases, the audit work is supervised by a different person who is performing the supervision and who has the proper accesses. If we do not have the proper accesses for adequate supervision, we disengage.

(U//~~FOUO~~)

(U//~~FOUO~~) DoD IG Finding: As a result, classified and SAP contracts are DoD OIG: (b) [redacted]. (Report, page 1, Findings)

(U) DCAA Comment: We disagree with this finding. The DoD IG did not identify any security or audit concerns that substantiate this finding.

Enclosure 1
(Response to Findings)
Page 5 of 5

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//

OIG Draft Report- Project No. D20 15-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017

(U) DoD IG Recommendation: We recommend that the Director, Defense Contract Audit Agency (DCAA): *(Report, page 18, Recommendation A.2)*

a. (U) Review and evaluate the leadership and performance of the Regional Director of FD, and report on what, if any management action has been taken.

(U) DCAA Comment: DCAA concurs with this recommendation. On November 18, 2016, which was during the course of your audit, the DCAA Director made a decision to reassign the FD Regional Director to perform a special project and the FD Deputy Regional Director was appointed as Acting FD Regional Director until such time as the position is filled on a permanent basis. [REDACTED] and [REDACTED] of your office were informed of this decision by the Acting Regional Director via email on November 22, 2016 and this was subsequently discussed with you at a meeting on December 14, 2016.

b. (U) Designate FD security duties to a qualified security official.

(U) DCAA Comment: DCAA concurs in principle with this recommendation. DCAA FD has always maintained a highly trained and qualified cadre of security specialists. Effective January 1, 2016, all security functions were centralized under the Agency Security Officer who reports to the Human Capital and Resources Management Directorate. On April 22, 2016, the DCAA Agency Security Officer received a letter from the SAPCO appointing her as the DCAA Government Special Security Officer (GSSO).

c. (U) In coordination with the Defense Contract Audit Agency Security Office develop and implement a formalized program access request process to initiate, approve, debrief, and maintain personnel accesses.

(U) DCAA Comment: DCAA concurs with this recommendation. Effective February 1, 2017, Security formalized the PAR process to initiate, approve, debrief, and maintain personnel accesses. This includes a new PAR form which is already being used and a standard operating procedure (SOP) which we plan to issue by June 2017. On April 27, 2017 CS will brief all FD management on the new process.

d. (U) Authorize property accountability officials to update property accountability files.

(U) DCAA Comment: DCAA concurs with this recommendation. All FD trained and certified property custodians are currently authorized to access accountability files and property systems. FD complies with DCAA Instruction 5000.17, DCAA Property Management Program previously provided to your office. In May 2016, all FD property custodians received property management training. This training included how to

Enclosure 2
(Response to Recommendations)
Page 1 of 12

UNCLASSIFIED//

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED// [REDACTED]

OIG Draft Report- Project No. D20 15-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017

appropriately utilize DPAS and ensure data input is accurate. DCAA was advised by your office that we would be given the opportunity to meet face to face to get clarification of the findings. This meeting never occurred.

c. (U) Dispose of damaged and excess equipment.

(U) **DCAA Comment:** DCAA concurs with this recommendation. During GFY 2016 and 2017, every FD FAO removed all damaged and excess property in accordance with DCAA Instruction 5000.17.

(U//~~FOUO~~)

f. (U) [REDACTED] Initiate corrective action to the 2012 Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office Staff Assistance Visit report.

(U) [REDACTED] **DCAA Comment:** DCAA concurs with this recommendation. FD Security provided a response on August 6, 2012 to the above referenced SAV. In response, the SAPCO provided assistance by detailing two Program Security Officers (PSOs) to DCAA to assist in implementing corrective actions. Actions were taken to identify the corrections necessary and in 2015 FD established the Business Process Integration Team (BPIT) to address several security issues not previously resolved. In February 2017, we have established a team dedicated to address audit and security requirements for Field Detachment. At the end of this team's assessment, to be completed December 31, 2017, audit and security policies and procedures will be established to ensure compliance with DoD directives, policies, and guidelines for safeguarding and protecting classified information.

(U) [REDACTED] **DoD IG Recommendation:** We recommend that the DCAA Security Officer (*Report, page 18-20, Recommendation A.3*):

(U//~~FOUO~~)

a. (U) [REDACTED] Identify and complete all required co-utilization agreements for the Defense Contract Audit Agency Field Detachment.

(U) **DCAA Comment:** DCAA concurs with this recommendation. In 2014, FD started conducting assessments to determine the need for co-utilization agreements at our various locations. These assessments were done in conjunction with SAPCO personnel detailed to the FD Security Office in response to the May 2012 SAV report. FD has a current co-utilization agreement for the Regional Office and DCAA.

[REDACTED]. Specifically, this co-utilization agreement covers DoD OIG: Branch Office DoD OIG: DoD Branch Office DoD DoD OIG: Branch Office DoD DoD OIG: (b) Branch Office DoD), NRO: (b) (3), OIG: (b) and DoD OIG: (b) (7)(E) Branch Office DoD) in addition to the regional office.

Enclosure 2
(Response to Recommendations)
Page 2 of 12

UNCLASSIFIED// [REDACTED]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED// [REDACTED]

OIG Draft Report- Project No. D20 15-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017

(U//~~FOUO~~) DCAA Comment: In April 2016, the Security Office

NRO: (b) (3), 10 USC § 424
[REDACTED]

(U//~~FOUO~~)

b. (U// [REDACTED]) Update internal guidance to require classification reviews from the customer program security officer for audit work derived from classified information.

(U) DCAA Comment: DCAA concurs in part with this recommendation. DCAA does not agree that classification reviews of documents containing information extracted from other classified documents is required. This report mischaracterizes the DCAA process. The DoD IG did not provide any evidence or example of any documents that were not appropriately marked. FD auditors are not original classifiers, we are derivative classifiers. DoD Manual 5200.01, Volume 1 dated February 24, 2012 states,

When incorporating, paraphrasing, restating, or generating classified information in a new form or document (i.e., derivatively classified information) ... Within the Department of Defense all cleared personnel, who generate or create material that is to be derivatively classified, shall ensure that the derivative classification is accomplished in accordance with this enclosure. No specific, individual delegation of authority is required. DoD official who sign or approve derivatively classified documents have principal responsibility of the quality of the derivative classified.

(U) The FD supervisor/manager validates that DCAA documents are appropriately classified by using the source document, consulting with the originator of the document or consulting with the Agency security office.

(U) As derivative classifiers, we follow DoD 5200.01 Volume 1 under Procedures for Derivative Classification that states:

a. *Derivative Classifiers shall carefully analyze the material they are classifying to determine what information it contains or reveals and shall evaluate the information against the instruction provided by the classification guidance or the marking on source documents ...*

Enclosure 2
(Response to Recommendations)
Page 3 of 12

UNCLASSIFIED// [REDACTED]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED// [REDACTED]

OIG Draft Report- Project No. D2015-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017

e. If extracting information from a document or section of a document classified by compilation, the derivative classifier shall consult the explanation on the source document to determine the appropriate classification. If that does not provide sufficient guidance, the derivative classifier shall contact the originator of the source document for assistance.

(U) We agree that if a document is not appropriately portioned marked we will direct our auditors to coordinate with the customer PSO. We will update our procedures to include this step and reiterate the importance to contact the appropriate PSO if they have any questions concerning the classification of a document.

(U//~~FOUO~~)

c. (U// [REDACTED]) **Develop and implement an incident response plan, including updated policies and procedures, for reporting, tracking, and investigating Field Detachment security incidents.**

(U) **DCAA Comment:** DCAA concurs with this recommendation. Prior to August 2014, the security incident log was maintained on FD DoD OIG: (b) (7)(E) [REDACTED] is no longer being utilized, therefore that data is unavailable. Between August 2014 and January 2016, FD maintained an informal incident log DCAA: (b) (7)(E) [REDACTED].

(U) **DCAA Comment:** In January 2017, the Security Office (CS) implemented a new process and a Standard Operating Procedure (SOP) has been developed for reporting, tracking, and investigating DCAA security incidents. Only the Security office has access to the security incident database. Copies of the SOPs and the security incident form are available upon request. Notification has been forwarded to the affected employees. Refresher training will be provided on April 27, 2017 to all FAO Security Control Officers (SCOs).

d. (U// [REDACTED]) **Update the SF 700s with the required information and limit access to the special access programs DoD OIG: (b) (7)(E) [REDACTED] to those who are approved for access.**

(U) **DCAA Comment:** DCAA concurs with this recommendation. A memorandum was forwarded to each individual FAO on October 7, 2016 for corrective action on this recommendation. By December 2017, we plan to validate that this has been completed.

(U) **DCAA Comment:** The Security Office will require all FD FAOs to complete and submit updated SF 700s by December 2017. Additionally, the Security Office will conduct a review of the SF 700s annually.

Enclosure 2
(Response to Recommendations)
Page 4 of 12

UNCLASSIFIED// [REDACTED]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED// [REDACTED]

OIG Draft Report- Project No. D2015-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017

e. (U// [REDACTED]) Implement the use of authorized access lists and visitor logs in Defense Contract Audit Agency Field Detachment computer server rooms.

(U) DCAA Comment: DCAA concurs with this recommendation. DCAA has a long range project to consolidate servers which will address this recommendation. In the interim, DCAA plans to implement the utilization of access lists and visitor logs in our current server rooms/cages by December 2017.

f. (U) Appoint its Government Special Security Officer (GSSO) in writing.

(U) DCAA Comment: DCAA concurs with this recommendation. On April 22, 2016, the DCAA Agency Security Officer received a letter from the SAPCO appointing her as the DCAA Government Special Security Officer (GSSO). An Alternate GSSO will be appointed in writing by the GSSO by April 30, 2017.

(U//~~FOUO~~)
g. (U// [REDACTED]) Complete special access program facility accreditation documentation for the Defense Contract Audit Agency Field Detachment locations.

(U//~~FOUO~~) DCAA Comment: DCAA concurs in principle with this recommendation. DCAA does not have accreditation authority however; each location has a site folder which contains accreditation documentation. NRO: (b) (3), 10 USC § 424 [REDACTED] By December 2017, we plan to visit each site to review data in the site folders for accuracy and completeness.

(U//~~FOUO~~) DCAA Comment: We are requesting the DoD IG provide clarification on the finding as it relates to physical security and the protection of classified material that is currently located within a Sensitive Compartmented Facility (SCIF). We are aware of the Co-Utilization Agreement requirement NRO: (b) (3), 10 USC § 424 [REDACTED] but we are not clear as to what additional physical security enhancements are required for our SCIF locations.

h. (U// [REDACTED]) Work with the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office to identify all Field Detachment personnel special access program accesses.

(U// [REDACTED]) DCAA Comment: DCAA concurs with this recommendation. In March 2016, based on the JADE, the BPIT developed an unclassified database (the PID Database) of accesses by person for use by FD management. DoD OIG: (b) (7)(E) [REDACTED] The DCAA list is sorted in two different ways for ease of use. This database is available view-only to FD management. The

Enclosure 2
(Response to Recommendations)
Page 5 of 12

UNCLASSIFIED// [REDACTED]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED// [REDACTED]

OIG Draft Report- Project No. D2015-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment." March 2, 2017

Security Office is assessing the capability to utilize Security Information Management System (SIMS) to maintain this database. We will complete this action by January 2018.

(U) **DCAA Comment:** DCAA will continue to review and determine SAP access requirements. Security is working with the SAPCO to utilize JADE at alternate locations until the DCAA: (b) (7)(E) SCIF is accredited. Until such time, the security staff will continue to update JADE when available.

i. (U// [REDACTED]) **In coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office, develop and implement a formalized automated process to request, initiate, approve, debrief, and maintain personnel special access program accesses.**

(U) **DCAA Comment:** DCAA concurs with this recommendation. Effective February 1, 2017, Security formalized the PAR process to initiate, approve, debrief, and maintain personnel accesses. This includes a new PAR form and a Standard Operating Procedure (SOP). We believe this new process will be finalized by December 2017. DCAA is currently working with the DoD SAPCO on reviewing and updating JADE to ensure the appropriate SAP accesses are reflected.

1. (U// [REDACTED]) **Debrief all personnel that do not have a valid need-to-know, are not clearly and materially contributing to the oversight of the special access program, and no longer require access to the information.**

(U) **DCAA Comment:** DCAA concurs with this recommendation. As of March 2017, we removed approximately DoD accesses from JADE. We will complete the analysis by September 2017. We will continue to conduct debriefs and update JADE when the system is available.

2. (U// [REDACTED]) **Develop and maintain a special access program master list, and provide site specific access list to the Field Detachment security managers.**

(U//FOUO) **DCAA Comment:** DCAA concurs with this recommendation. We have developed and are currently maintaining a transitional database DoD OIG: (b) (7)(E) of all DCAA accesses. The DoD list is available on the shared drive for the Field Audit Office (FAO) Managers.

(U) **DCAA Comment:** Security is in the development phase of utilizing an automated system (i.e. SIMS), which will enable Security to run reports that will provide site specific accesses to DCAA FAO Managers. We will complete this action by January 2018.

Enclosure 2
(Response to Recommendations)
Page 6 of 12

UNCLASSIFIED// [REDACTED]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//

OIG Draft Report- Project No. D2015-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017

3. (U//) Require security managers to destroy the old document when they receive an updated list.

(U) DCAA Comment: Field visits are planned to validate that FAOs are using the most current JADE reports and are appropriately destroying outdated reports. We will complete this action by September 2017.

4. (U) Inform the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office of all updates to DoD DCAA: (b) (7)(E) accesses.

(U) DCAA Comment: DCAA partially concurs with this recommendation. DCAA concurs that DoD program accesses for DCAA personnel will be in JADE and the SAPCO is involved in the current approval process for new DoD program accesses under their cognizance. DCAA does not concur that providing information DCAA: (b) (7)(E) to unauthorized individuals is appropriate. We request further clarification from the DoD IG on the policy requirements for providing DoD OIG: accesses to SAPCO.

- j. (U) Update, complete, sign, and disseminate security policies and procedures.

(U) DCAA Comment: DCAA concurs with this recommendation. DCAA is in the processes of developing and updating security policies and procedures. We will complete this action by March 2018.

- k. (U) Develop a separate automated accountability systems for Top Secret collateral and SAP material. The accountability system must be standardized and include the minimum required information found in the DoD Manual 5200.00, volume 1, "DOD Information Security Programs, Overview, Classification, and Declassification, February 24, 2012."

(U) DCAA Comment: DCAA concurs with this recommendation. DCAA is in the process of deploying SIMS. SIMS has the capabilities to maintain and report accountable and controlled classified material. We plan to complete this task by January 2018.

- l. (U) Work with the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office to identify and grant access to the Top Secret Control Officers, alternate Top Secret Control Officers, and the designated disinterested persons responsible for the accountability systems.

(U) DCAA Comment: DCAA concurs with this recommendation.

Enclosure 2
(Response to Recommendations)
Page 7 of 12

UNCLASSIFIED//

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//

●IG Draft Report- Project No. D2015-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017

Security and the Program Action Response Team will conduct a review of the classified holdings. The feedback from this review will determine the requirement to designate a TSCO/ATSCO at specific locations. DCAA's Security Office is developing TSCO training to be delivered to the designated TSCOs by December 2017.

m. **(U) Require all Defense Contract Audit Agency personnel performing audits of classified and special access program contracts receive mandated training and track all training.**

(U) **DCAA Comment:** DCAA concurs in principle with this recommendation. In the past DCAA FD personnel did participate in the three-day Defense Security Service SAP Introduction Course which is designed for the GS-080 Security Specialist series. However, this course was designed for security professionals and was not beneficial to DCAA auditors. Therefore, DSS tailored the course and provided the training to FD personnel; however, it was discontinued a few years ago.

(U) The DCAA Security Office is developing SAP orientation training which will be incorporated into the Agency's learning management system. DCAA will implement refresher training upon receipt from the SAPCO. We will complete this project by December 2017.

n. **(U) Initiate corrective action based on the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office risk assessment.**

(U) DCAA concurs with this recommendation. DCAA will participate in any risk assessment performed by the SAPCO. Completion of this recommendation will be based on the dates the corrective actions are received from SAPCO.

(U) DoD IG Recommendation: We recommend that the Director, Defense Contract Audit Agency (DCAA): (Report, page 26-27, Recommendation B.1)

a. **(U) Ensure special access program contract audits are included in Defense Contract Audit Agency annual planning guidance.**

(U) **DCAA Comment:** DCAA concurs in principle with this recommendation. The Agency's yearly staff allocation and future plan guidance addresses all of DCAA's unclassified and classified workload. It does not separately identify classified work as a top planning priority; rather identifies types of priority audits which FD uses to plan the audit effort for contractors under its cognizance and coordinate the completion of the direct cost audits of SAP/SCI contracts with the cognizant Regional DCAA FAO. In fact, it is not in our control to know all classified contracts issued. Ultimately, it is the contracting officer's responsibility to

Enclosure 2
(Response to Recommendations)
Page 8 of 12

UNCLASSIFIED//

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

OIG Draft Report- Project No. D2015-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017

notify DCAA of contract awards as stated in FAR chapter 4.2; however, FD employees have many processes to identify SAP work.

b. (U) Notify all DCAA employees that the Field Detachment is responsible for performing all audit assignments involving classified and special access program contracts.

(U) DCAA Comment: DCAA does not concur with this recommendation. The DoD IG is implying that cleared people must perform all audits that may impact classified and special access program contracts whether the audit effort is unclassified or classified. We request another meeting with the DoD IG to further explain our operations. We attempted to explain to the DoD IG the infeasibility of this recommendation during our previous meeting to the discussion draft. FD is responsible for performing the parts of the audit assignment involving access to classified information (i.e. direct cost). Uncleared auditors are aware that FD is the organization that must be contacted if clearances are required to appropriately complete an audit step or perform an audit. To reiterate DCAA's policy, FD leadership will attend scheduled supervisory workshops across the Agency where we will brief all management on FD's mission and responsibilities in June and July 2017.

c. (U) Establish an Agency wide process requiring auditors to review the DD Form 254, "DoD Contract Security Classification Specification," as part of the program audit plan before performing a review of the contract.

(U) DCAA Comment: DCAA partially concurs with this recommendation. DCAA does not agree that the existence of a DD Form 254 automatically means a cleared auditor is required to perform the audit. However, DCAA agrees the DD Form 254 indicates potential contracts that require further review by cleared personnel to make a determination. All auditors are aware that FD is the organization that will perform audit work that requires clearances. This will be a topic during the supervisory workshops as discussed as discussed above.

d. (U) Based on the results of recommendation B.I.C (above) notifies the Field Detachment of all classified, sensitive compartmented information, and special program related efforts.

(U) DCAA Comment: DCAA concurs with this recommendation that FD should be notified of all classified, SCI and SAP contract efforts. We do not believe that reviewing a DD Form 254 solely accomplishes this effort. We will prepare training for all Agency supervisory auditors on what to do when classified contracts are identified during an audit. This training will be given at supervisory auditor workshops in June and July 2017.

Enclosure 2
(Response to Recommendations)
Page 9 of 12

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

OIG Draft Report- Project No. D2015-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017

(U) DoD IG Recommendation: We recommend that the Regional Director, Defense Contract Audit Agency (DCAA) Field Detachment (FD): *(Report, page 27-28, Recommendation B.2)*

a. **(U) Perform an annual assessment of Field Detachment staffing and facility requirements for audit oversight of classified and special access programs operations based on established criteria.**

1. **(U) The criteria must include: the volume of classified and special access programs workload at each site; the number of cleared personnel; and future audit requirements.**
2. **(U) The team should include involvement from Defense Contract Audit Agency Security Division and staff of equivalent responsibilities and authority.**
3. **(U) Identify and grant access to those Field Detachment employees designated to perform audits of classified and special access programs.**

(U) DCAA Comment: DCAA concurs with this recommendation. FD has always performed an annual assessment of staffing and facility requirements to adequately perform their mission. Recently FD established a program access response team which includes the Agency Security Division, to address future facility requirements and SCI/SAP needs for auditors. This team is expected to complete its mission by December 2017.

b. **(U) Establish and implement a process for annual planning and coordination with customer program security officers and Field Detachment supervisors to identify classified and special access programs.**

(U//FOUO) DCAA Comment: DCAA concurs in principle with this recommendation. FD does have a process for identifying SAP contracts. FD employs many techniques to identify classified workload and having to coordinate with every customer program security officer would place an undue burden on DCAA since we support hundreds of programs. FD leadership has placed emphasis on meeting the customers' needs in many ways. FD has established ^{DoD}_{OIG} customer-centric audit teams to address the audit needs of the command expediently. FD leadership has assigned Financial Liaison Advisors (FLAs) at many of the commands with classified work. The FLAs expedite the communication and planning between the program office and the auditors. We will coordinate with the AT&L SAPCO to explore the possibility of coordinating with individual SAPCOs of major DoD components to obtain information that would assist us in identifying contracts, however, ultimately it is the contracting officer's responsibility to notify DCAA of contract awards as stated in FAR chapter 4.2.

Enclosure 2
(Response to Recommendations)
Page 10 of 12

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

OIG Draft Report- Project No. D2015-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017

1. (U) Work with Defense Contract Audit Agency Security Officer and the Under Secretary of Defense for Acquisition, Technology, and Logistics Special Access Program Central Office, to designate a group of Field Detachment leadership and branch managers, to receive access to special access programs to conduct planning and oversight.

(U) DCAA Comment: DCAA does not concur with this recommendation. This is contrary to the direction of the SAPCO and the NRO, Director, Office of Security and Counterintelligence, to limit SCI/SAP accesses and secure facilities. We recommend that the IG, AT&L SAPCO and DCAA meet to resolve this issue since it would significantly increase the number of accesses throughout FD.

2. (U) Conduct annual planning to identify Field Detachment audit oversight efforts for classified and special access programs projects.

(U) See b. above.

3. (U) Reassess the use of regular telework schedules to ensure adequate personnel are available to audit classified and SAP contracts.

(U) DCAA Comment: DCAA does not concur with this recommendation. We believe this issues stems from the DoD IG's believe that all audit effort performed at a contractor with a classified contract is also classified. Unclassified audit effort exists even though the contract may have some classified contracts. A DCAA employee is eligible to telework when his/her position has some duties considered portable that can be performed at the alternate location and his/her performance and conduct meet the criteria required by the DoD and DCAA instructions. In determining portable work, the auditor and supervisor must consider the classification of the information required. For example, often times information obtained from a contractors accounting system is unclassified and allows the auditor to perform analysis, sampling and testing at alternate locations.

4. (U) Determine annually whether classified, sensitive compartmented information and special access programs are receiving adequate audit oversight.

(U) DCAA Comment: DCAA concurs in principle. As stated in part b., above it is part of our planning process to identify and audit contractor processes and claimed costs impacting classified contracts.

Enclosure 2
(Response to Recommendation(s))
Page 11 of 12

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Defense Contract Audit Agency (cont'd)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED// [REDACTED]

OIG Draft Report- Project No. D2015-DISPA3-0248.00, "Audit of Defense Contract Audit Agency Field Detachment," March 2, 2017


c. (U) **Acquire and use a classified automated information system for conducting classified audit assignments and reports.**

(U) **DCAA Comment:** DCAA does not concur with this recommendation. DCAA needs to perform a cost/beneficial assessment of the feasibility of this recommendation. We will work with the SAPCO to perform this assessment. However, your draft report indicates that DCAA personnel are creating audit working papers on a DoD OIG: (b) (7)(E) [REDACTED] which is not correct. DCAA does in some cases have DoD OIG: (b) (7)(E) [REDACTED]. This information is read only DoD OIG: (b) (7)(E) [REDACTED]. Currently, offices are using DoD OIG: (b) (7)(E) [REDACTED]. We do not believe that utilizing DoD OIG: (b) (7)(E) [REDACTED].

UNCLASSIFIED// [REDACTED]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) Acronyms and Abbreviations

| | |
|----------------------------|---|
| BPIT | Business Process Implementation Team |
| DCAA | Defense Contract Audit Agency |
| FAO | Field Audit Office |
| FD | Field Detachment |
| PAR | Program Access Request |
| SAP | Special Access Program |
| SAPCO | Special Access Program Central Office |
| DoD OIG: (b) (7)(E) |  |
| SCIF | Sensitive Compartmented Information Facility |
| TSCO | Top Secret Control Officer |

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 Hotline Director. For more information on your rights and remedies against retaliation, visit 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

Media Contact

public.affairs@dodig.mil; 703.604.8324

For Report Notifications

http://www.dodig.mil/pubs/email_update.cfm

Twitter

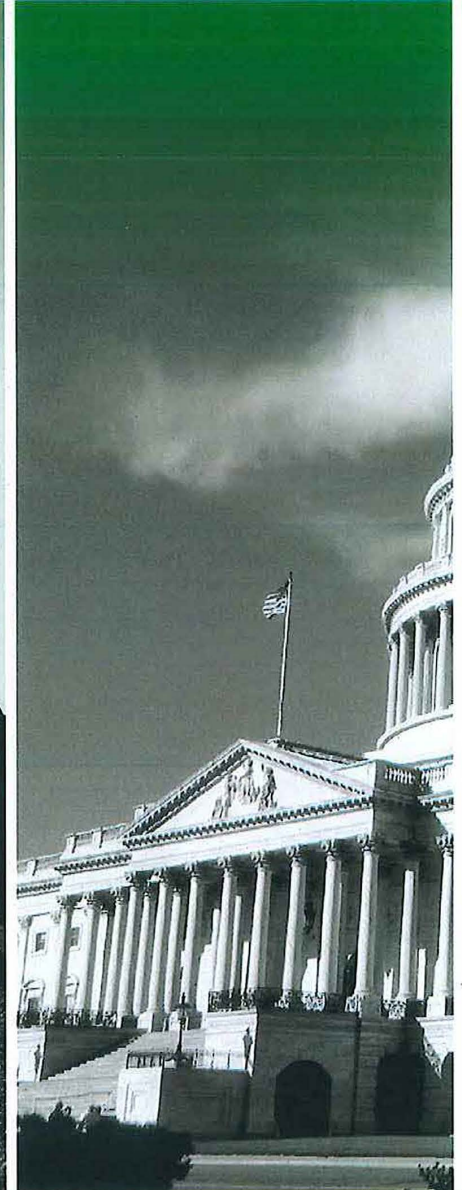
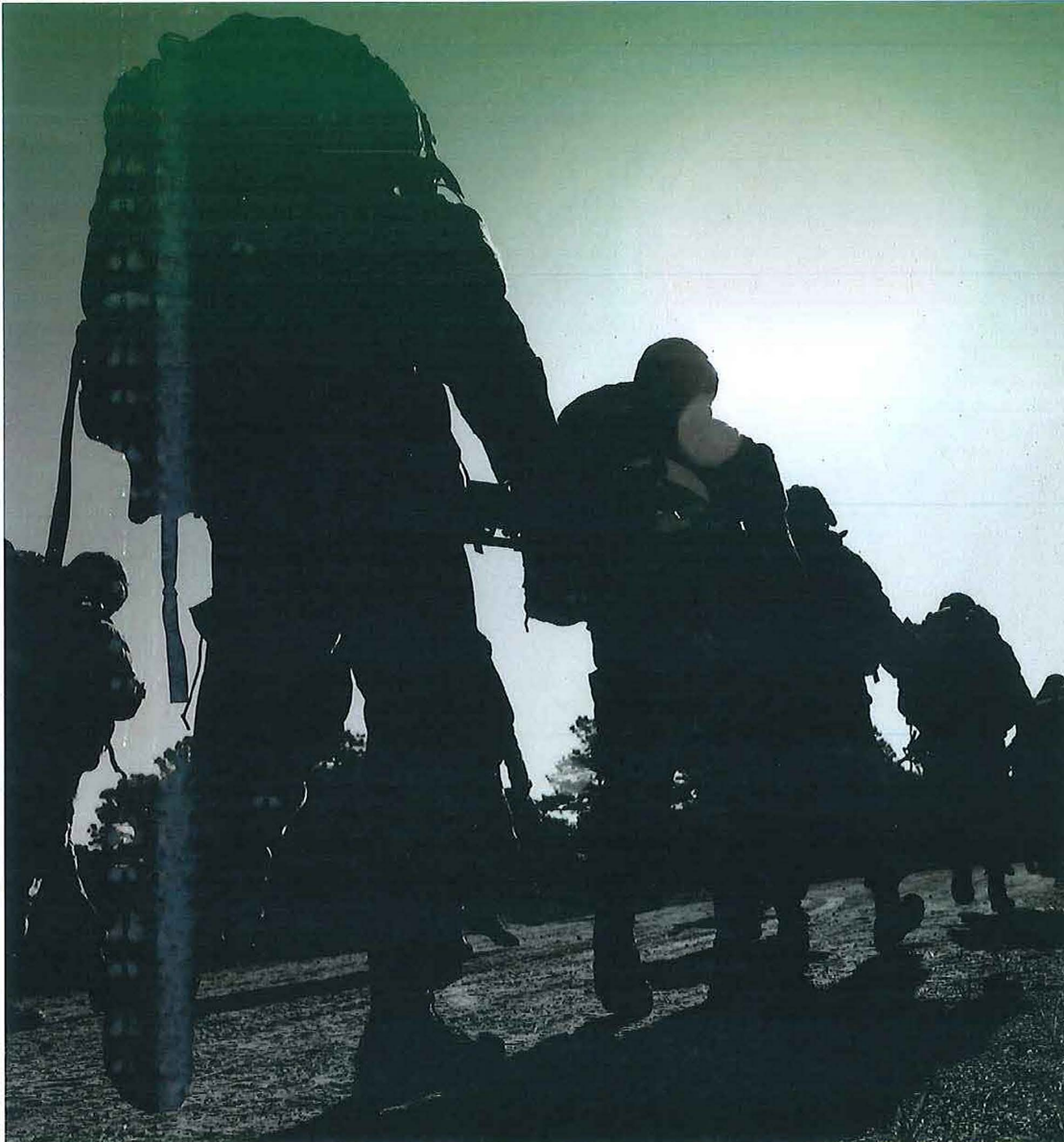
twitter.com/DoD_IG

DoD Hotline

dodig.mil/hotline

~~FOR OFFICIAL USE ONLY~~

~~DISTRIBUTION D: Distribution authorized to Department of Defense and US DoD Contractors Only (Vulnerability Information). Other requests for this document will be referred to the DoD Inspector General~~



DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098

~~FOR OFFICIAL USE ONLY~~