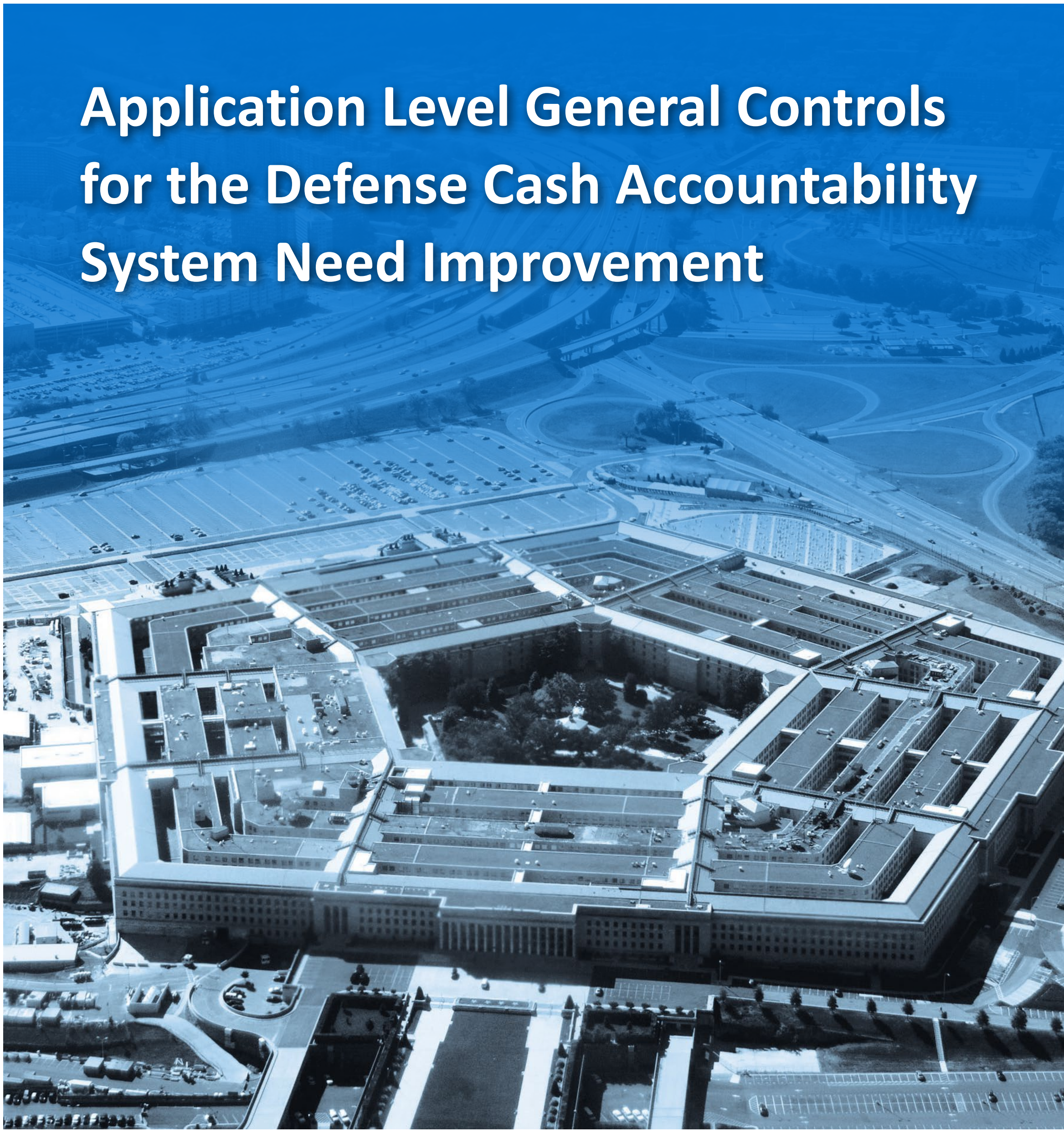
Report No. DODIG-2017-015

Inspector General

U.S. Department of Defense

NOVEMBER 10, 2016

Application Level General Controls for the Defense Cash Accountability System Need Improvement



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

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.

Fraud, Waste, & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline | 800.424.9098

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

Results in Brief

Application Level General Controls for the Defense Cash Accountability System Need Improvement

November 10, 2016

Objective

We determined whether Defense Cash Accountability System (DCAS) general controls including those related to security management, access controls, contingency planning, configuration management, and segregation of duties were operating effectively. DoD uses DCAS to process and report its disbursement and collections of funds between the U.S. Treasury and DoD.

Findings

DCAS general controls administered by the Defense Finance and Accounting Service (DFAS) did not operate effectively. Specifically:

- Business Enterprise Information Services (BEIS) Office personnel did not properly approve and train Information System Security Officers or review compliance with the service level agreement[1] (Security Management);
- DCAS authorizing officials did not review user permissions for continued appropriateness of user access, including permission for users with access to sensitive financial data (Access Controls);

Findings (cont'd)

- BEIS Office personnel did not coordinate or update the DCAS Information System Contingency Plan, and they did not update the Business Continuity Plans, Disaster Recovery Plans, and Continuity of Operations Plans to correct deficiencies identified during internal contingency plan testing (Contingency Planning); and
- BEIS Office personnel did not control developer access to DCAS source code in the test environment, track authorized system changes made to DCAS, or properly identify DCAS emergency changes,[2] and document what those actions were and how they should have been implemented (Configuration Management).

These controls did not operate effectively because BEIS Office personnel did not follow the DCAS Access Control Policy, ensure comprehensive procedures existed, or train DFAS staff effectively. As a result, DCAS had an increased risk that users accessed DCAS without authorization or correct level of privileges. In addition, the control weaknesses identified could circumvent segregation of duties[3] controls, which were operating as intended.

Without proper controls, DCAS is vulnerable to availability interruptions and lost or incorrectly processed data. Losing the capacity to process, retrieve, and protect electronically maintained data can significantly affect DoD's ability to accomplish its mission. DoD could consequently suffer financial losses, expensive recovery efforts, and inaccurate or incomplete information.

[1] A Service Level Agreement is a formal contract between all parties which defines their roles and responsibilities, a description of the service environment, service levels and costs, compliance and remedies for noncompliance, and period of performance.

[2] An emergency change is defined as a critical system discrepancy that prohibits the application or system from running successfully, causes significant errors, affects critical data accuracy, or compromises security.

[3] Work responsibilities should be segregated so that one individual does not control all critical stages of a process. For example, while users may authorize program changes, programmers should not be allowed to do so because they are not the owners of the system and do not have the responsibility to see that the system meets user needs.

Visit us at www.dodig.mil

Results in Brief

Application Level General Controls for the Defense Cash Accountability System Need Improvement

Recommendations

The Director of BEIS and Other Systems, DFAS, should clearly identify user access privileges, properly coordinate the DCAS contingency plan, remove access in a timely manner from terminated developers, develop a formal Information Assurance training policy, develop procedures to require Information System Security Officers to obtain and retain DoD-required certifications, and develop a process to review service provider compliance with the Service Level Agreement.

Management Comments and Our Response

Comments from the Director, Information and Technology, DFAS, responding for the Director of BEIS and Other Systems, DFAS, addressed the recommendations to comply with certification requirements, review compliance, provide training on policy and system access, develop and document procedures on approved users, fix discrepancies, and update the Vulnerability Management Plan. However, the Director partially addressed the specifics of the recommendations to provide training on monitoring responsibilities, implement policy for training plans, incorporate lessons learned into the contingency plan, remove system access in a timely manner, and monitor changes in DCAS. We request additional comments to this report by December 12, 2016. Please see the Recommendations Table on the next page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Director of Business Enterprise Information Services and Other Systems, Defense Finance and Accounting Service	A.1.a, A.1.b, B.1.d, C.1.a, C.1.b, D.1.a.1, D.1.a.2, D.1.a.4	A.1.c.1, A.1.c.2, A.1.d, B.1.a, B.1.b, B.1.c, B.1.e, B.1.f, B.1.g, D.1.a.3, D.1.b, D.1.c

Management Comments due by December 12, 2016.

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

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

November 10, 2016

MEMORANDUM FOR CHIEF INFORMATION OFFICER, DEFENSE FINANCE AND
ACCOUNTING SERVICE
DIRECTOR OF BUSINESS ENTERPRISE INFORMATION SERVICES AND
OTHER SYSTEMS, DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Application Level General Controls for the Defense Cash Accountability System Need Improvement (Report No. DODIG-2017-015)

We are providing this report for review and comment. Defense Cash Accountability System (DCAS) needs improved controls over security management, access controls, contingency planning, and configuration management. Without effective controls, the Defense Finance and Accounting Service (DFAS) cannot ensure that its financial transactions between the U.S. Treasury and DoD are complete, valid, confidential, and available. Although the information we analyzed was from October 2014 through March 2015, it is relevant for DFAS to ensure that the DCAS general controls are operating effectively because the reliability of financial data processed in DCAS is vital to the success of the financial statement audits across DoD. We conducted this audit in accordance with generally accepted government auditing standards.

We considered management comments on a draft of this report when preparing the final report. DoD Instruction 7650.03 requires that all recommendations be resolved promptly. Comments from the Director, Information and Technology, DFAS, responding for the Director of Business Enterprise Information Services and Other Systems, DFAS, partially addressed the recommendations. We request additional comments on Recommendations A.1.a, A.1.b, B.1.d, C.1.a, C.1.b, D.1.a.1, D.1.a.2, and D.1.a.4 by December 12, 2016.

Please send a PDF file containing your comments to audclev@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 601-5945 (DSN 664-5945).

Lorin T. Venable

Lorin T. Venable, CPA
Assistant Inspector General
Financial Management and Reporting

Contents

Introduction

Findings

Contents (cont'd)

Appendix

Management Comments

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

Introduction

Objective

We determined whether Defense Cash Accountability System (DCAS) general controls[4] including those related to security management, access controls, contingency planning, configuration management, and segregation of duties were operating effectively. See the Appendix for the scope and methodology and prior audit coverage.

Background

DoD uses DCAS to process and report its disbursement and collections of funds to the U.S. Treasury and DoD. DCAS receives financial transaction data recorded from various DoD entity feeder systems, validates and checks the accuracy of the data, and sends the data to appropriate DoD entity accounting systems. Additionally, DCAS prepares reports[5] for DoD accounts referred to as Fund Balance With Treasury.[6] DCAS processes about 4,730,000 transactions and averages 18,300 corrective adjustments each month.

The Defense Finance and Accounting Service (DFAS) identified that DCAS is a system that processes disbursement and collection transactions that it deems necessary for day-to-day operations, but DCAS is not directly related to the support of deployed or contingency forces. In addition, DFAS has identified all information within DCAS as sensitive.

In October 2014[7] the ownership of DCAS began transitioning from the Defense Logistics Agency (DLA) to DFAS because DCAS had reached the sustainment phase of its lifecycle. As part of the transition, the DFAS Chief Information Officer agreed that the DFAS Director of BEIS and Other Systems (BEIS Office) would maintain and monitor the security posture of DCAS. The complete transition of DCAS from DLA to DFAS occurred in October 2015.

[4] We refer to these controls in the report as the application level general controls.

[5] Financial Management System 1219 Statement of Accountability and 1220 Statement of Transactions reports.

[6] Fund Balance With Treasury is an asset account that reflects the available budgetary spending authority of a Federal agency. Fund Balance With Treasury is similar to a corporation's cash account.

[7] "Memorandum of Understanding Between the Defense Finance and Accounting Service and the Defense Logistics Agency for the Business Enterprise Information Services Family of Systems Transfer of Cybersecurity Responsibility," October 2014.

Information System Security Controls

Each Federal agency is required to comply with Federal Information Security Modernization Act (FISMA)[8] and related policies, procedures, standards, and guidelines, including the information security standards stated under section 11331, title 40, United States Code (40 U.S.C. § 11331). Standards and guidelines for Federal information systems are to be based on standards and guidelines developed by the National Institute of Standards and Technology (NIST).

Information system controls are generally divided into two categories: general and application level general controls. General controls are applied at the entity-wide, system, and application levels. Business process application general controls include:

- security management controls that provide a framework to manage risk, develop security policies, assign responsibilities, and monitor the adequacy of the entity's application-related controls.
- access controls that are used to ensure authorized personnel have access to the application and only for authorized purposes.
- configuration management controls that assess changes to information systems to ensure changes are authorized so systems are configured and operated securely and as intended.
- contingency plans and procedures that support the operation and assets of the agency to minimize potential damage and interruptions.
- segregation of duties designed to prevent the possibility that a single person could be responsible for diverse and critical functions in such a way that errors or misappropriations could occur and not be detected in a timely manner, in the normal course of business processes.

Security Control Guidelines

NIST Special Publication 800-53[9] stipulates the guidelines that apply to all Federal information systems.[10] It provides a catalog of security and privacy controls for Federal information systems and organizations and a process for selecting controls to protect organizational operations and assets, individuals, other organizations, and the nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors. These NIST controls are tested using the Government Accountability Office (GAO) Federal Information

[8] Public Law 113-283, "Federal Information Security Modernization Act of 2014," December 18, 2014.

[9] NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, April 2013, including updates as of January 22, 2015.

[10] Excludes national security systems as defined by 44 U.S.C § 3542.

System Controls Audit Manual (FISCAM). We used the GAO FISCAM controls to evaluate the effectiveness of general and application controls. See the Appendix for additional information on the scope and methodology.

Review of Internal Controls

DoD Instruction 5010.40[11] 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. Although we did not identify control weaknesses with segregation of duties,[12] we did identify internal control weaknesses associated with security management, access controls, configuration management, and contingency planning. The control weaknesses identified could circumvent segregation of duties controls. We will provide a copy of the report to the senior official responsible for internal controls at DFAS.

[11] DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

[12] Work responsibilities should be segregated so that one individual does not control all critical stages of a process. For example, while users may authorize program changes, programmers should not be allowed to do so because they are not the owners of the system and do not have the responsibility to see that the system meets user needs.

Finding A

Application Security Management Needs to Be Strengthened

Effective DCAS security management provides a basis for BEIS Office personnel to obtain reasonable assurance that DCAS is effectively secure. However, the DCAS general controls related to security management were not operating effectively. Specifically:

- BEIS Office personnel did not establish a policy to implement requirements for an Information Assurance (IA) Training, Certification, and Workforce Management program. This occurred because the BEIS Office personnel did not document their internal policies and procedures for IA training requirements. As a result, management's requirements or actual intent was not known and could not be enforced.
- BEIS Office personnel did not approve DCAS Information System Security Officers (ISSOs) in accordance with DCAS's access control policy (ACP). This occurred because BEIS Office personnel did not implement the procedures as defined in their ACP. As a result, DCAS had a greater risk for unauthorized access to sensitive data.
- The DCAS ISSOs did not obtain DoD-required certifications[13] to be a designated ISSO. This occurred because BEIS Office personnel did not have processes to verify ISSOs met DoD certification requirements. As a result, DCAS had a greater risk for unauthorized access to sensitive data.
- BEIS Office personnel did not ensure that the Defense Information Systems Agency (DISA) complied with the services that were documented in the Service Level Agreement (SLA).[14] In addition BEIS Office personnel did not ensure that DISA complied with security policies and procedures. This occurred because BEIS Office personnel did not comply with NIST[15] requirements to develop a process that ensured its service provider, DISA, provided the services documented in the SLA for DCAS. As a result, DFAS did not have assurance that DISA complied with the terms of its SLA and that both DISA and DFAS's security procedures and policies were being followed.

[13] DoD 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, incorporating changes dated January 24, 2012, provides the certification requirements. This manual was updated in November of 2015. However for our review of the first and second quarters of FY 2015, the 2012 manual contained the applicable criteria and was used for this report.

[14] A Service Level Agreement is a formal contract between all parties which defines their roles and responsibilities, a description of the service environment, service levels and costs, compliance and remedies for noncompliance, and period of performance.

[15] NIST SP 800-35, "Guide to Information Technology Security Services," October 2003.

- BEIS Office personnel did not perform required annual reviews of their SLA to ensure DISA was providing agreed-upon services. This occurred because the personnel stated that they believed the agreement did not need to be reviewed or signed again for 3 years. As a result, necessary financial or service level changes may not occur, which could impact the performance of DCAS.

Without effective security management, BEIS Office personnel increased the risk that management, information technology staff, application owners, and users did not properly assess risk. Consequently, BEIS Office personnel may have implemented inappropriate or inadequate information security over DCAS.

Information Assurance Training Lacked Documented Policies and Procedures

BEIS Office personnel did not establish a policy implementing the requirements for an IA Training, Certification, and Workforce Management program. DoD Manual 8570.01 states:

> The Heads of DoD Components shall include requirements for IA training in all DoD Component and local policy and procedures as part of the IA program.
>
> The Heads of DoD Components shall establish, resource, and implement plans, policies, and processes to meet the requirements of DoD Directive 8570.1 "Information Assurance Training, Certification, and Workforce Management" and this Manual.

Although the BEIS Office used an automated process to monitor when a user's IA training was due, the process was not formally documented in policy. The BEIS Office used SharePoint to display a mandatory training page for DCAS users that showed the date of their last training and when refresher training was due. Additionally, a supervisor summary page alerted supervisors when a user did not complete the mandatory training. Automated e-mail notices were also sent to users reminding them of training that was due or past due.

The BEIS Office demonstrated how training was tracked individually, but it did not provide a comprehensive policy that instructed users of the requirement to complete the training annually, how training completion requirements were confirmed, and the consequences of noncompliance.

Informal policies and procedures lack the weight of authority provided by the written approval of a senior management official. The signature of a responsible authority provides clear evidence for employees and contractors that management is in agreement with the stated policies and procedures and that adherence to them is required. Without published and communicated IA training policy, employees may not know management's actual intent and BEIS Office managers may not be able to enforce compliance. BEIS Office management should develop a formal IA training policy for DCAS users. The policy should include the training requirements for all DCAS users, assign monitoring responsibilities, and inform employees of the consequences of not complying with the IA training policy. Once formalized, they should disseminate the IA security awareness training policies and procedures to all DCAS users.

ISSO Identification and Certification Needs Improvement

BEIS Office personnel did not approve their DCAS ISSOs and require the DCAS ISSOs to obtain required certifications.

Inconsistent ISSO Identification

BEIS Office personnel did not designate and approve DCAS ISSOs as required by the DCAS ACP. The ACP requires that each Center Administrator (CA) be an ISSO. ISSOs play a key role in assisting with application security activities and access controls, and are essential for the effective management of DCAS access.

In response to our request for a list of DCAS ISSOs, BEIS Office personnel manually created a list of 17 ISSOs. The list included the date that the ISSOs signed their appointment letters and the date they needed to obtain their DoD-required certifications. We used DCAS ACP ISSO criteria to compare the manually generated list to a DCAS-generated list and determined that:

- six DCAS CAs on the DCAS list were not on the manually prepared list.
- five additional personnel were on the manually prepared list but were not on the DCAS list.
- three employees on the DCAS list were assigned the roles of DCAS System Administrator[16] and DCAS System Security Officer.[17]
  - Only one of these employees was on the manually prepared list of ISSOs; however, this employee was not assigned the role of CA.
  - BEIS Office management did not explain why the remaining two employees assigned these roles were not on the manually prepared list.

[16] DCAS System Administrators assign ISSOs.

[17] DCAS System Security Officers register, monitor, terminate, and reinstate user access.

These inconsistencies occurred because the BEIS Office personnel did not implement the ISSO approval procedures that all CAs be an ISSO as required by the ACP. BEIS Office personnel stated that the ACP requirements for approving ISSOs were outdated and did not provide any further explanation. As a result, DCAS had a greater risk for unauthorized access to sensitive data. BEIS Office management should ensure that the ACP clearly describes who BEIS Office management will approve to serve as DCAS ISSOs and update the ACP as necessary.

BEIS Office personnel stated that the ACP requirements for approving ISSOs were outdated.

DoD-Required Certifications Not Obtained By ISSOs

DCAS appointed ISSOs did not obtain DoD-required IA certifications.[18] DoD established an IA Workforce Improvement Program that requires all military and Government civilian IA personnel achieve the certification requirements within 6 months of assignment of IA duties, unless a waiver is granted. Of the 17 DCAS appointed ISSOs on the manual list provided by BEIS Office personnel, 6 DCAS appointed ISSOs did not have the required IA certification. Four of the six DCAS appointed ISSOs did not complete their certification training within 6 months of their appointments. The remaining two DCAS appointed ISSOs had expired certifications. The BEIS Office personnel could not explain why these six DCAS appointed ISSOs did not comply with DoD policy.

This occurred because the BEIS Office did not have a process to verify whether ISSOs completed and retained the DoD-required certifications and training requirements. As a result, DCAS had a greater risk for unauthorized access to sensitive data because ISSOs did not maintain the technical competencies necessary for their position as system security officers. BEIS Office management should develop and implement procedures to require all ISSOs meet and retain the certification requirements established in DoD Manual 8570.01-M.

Reviews of Service Level Agreement Were Not Performed

The BEIS Office personnel did not ensure that DISA complied with the services documented in the SLA and with security policies and procedures. In addition, BEIS Office personnel did not conduct annual reviews of the SLA to validate that it accurately documented service requirements. NIST requires managers to develop

[18] DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, incorporating changes from January 24, 2012. This manual was updated in November of 2015. However for our review of the first and second quarters of FY 2015, the 2012 manual contained the applicable criteria and was used for this report.

a defined process on how they will assess the service provider's compliance with the service agreement, including due-date targets, rules, and other terms of the agreement. NIST also requires the managers to ensure that the service provider meets its stated service levels and complies with internal security policies and procedures. Furthermore, managers should conduct evaluations and document them through periodic reports, compliance reports, end user evaluations, or metrics.

DFAS and DISA Enterprise Services Directorate signed an SLA on August 29, 2012, documenting the services that DISA was required to provide to DFAS in support of DCAS. BEIS Office personnel stated that in lieu of conducting the SLA compliance review, DFAS distributed the DISA Statement on Standards for Attestation Engagements 16 reports[19] throughout DFAS. However, the reports did not meet the NIST requirements for reviewing an SLA. For example, the reports did not address, among other requirements, whether the data storage agreed to in the DCAS SLA was sufficient to meet the needs of its users. DFAS personnel acknowledged that they did not perform a compliance review of the SLA to determine whether DISA met established service level requirements. This occurred because BEIS Office personnel did not comply with NIST requirements to develop a process that ensured its service provider, DISA, provided the services documented in the SLA for DCAS. As a result, DFAS did not have assurance that DISA complied with the terms of its SLA and that both DISA and DFAS security procedures and policies were being followed.

In addition, NIST[20] and DFAS policy require that the SLA be reviewed to determine if any modifications or amendments are needed. DFAS policy[21] requires the Office of Primary Responsibility to perform an annual review for both mission and nonmission work agreements and document the review in a memorandum for record. However, DFAS officials did not annually review the SLA because they did not believe that the annual evaluations were required. In addition, DFAS officials stated that the agreement did not need to be signed for another 3 years. As a result, necessary financial or service level changes may not occur, which could impact the performance of DCAS. BEIS Office management should develop and implement procedures to comply with NIST SP 800-35. This includes assigning review responsibilities to ensure that service providers comply with

DFAS officials did not annually review the SLA because they did not believe that the annual evaluations were required.

[19] An SSAE 16 report provides an attestation on whether the controls related to the control objectives stated in management's description of the service organization's system were suitably designed and working effectively throughout the specified period.

[20] NIST SP 800-35, "Guide to Information Technology Security Services," October 2003.

[21] DFAS Instruction 4000.1-I, "Support Agreements and Mission Work Agreements," March 17, 2015.

the terms of the SLA. In addition, BEIS Office management should provide training to applicable DFAS personnel on the DFAS policy to review governance over support and mission work agreements and compliance with SLA requirements.

Other Matters of Interest

BEIS Office personnel did not enable DCAS to encrypt data, including financial data, transferred from its web server to its database.[22] DoD policy[23] requires that entities maintain the confidentiality, integrity, and availability of DoD unclassified information that has not been approved for public release. When transmitting data, such as from the web to a database, it is important that security of the information is maintained. To achieve the required security and maintain confidentiality of the system's information, it is a best business practice to encrypt sensitive information during transmission.

BEIS Office personnel stated that while they were able to encrypt data transferred between the web server and database, they did not deem it necessary for DCAS. They stated that because the public had no access to DCAS and the web and database servers were on a DoD secured network, encryption was not needed. However, if the DoD secured network is breached, DCAS data is at greater risk of exposure for misuse of data. As a best practice and in light of the 2015 Office of Personnel Management data breach, DFAS should encrypt this data transmission to ensure the data remains secure.

Recommendations, Management Comments, and Our Response

Recommendation A.1

We recommend that the Director of Business Enterprise Information Services and Other Systems, Defense Finance and Accounting Service:

a. **Develop a formal Information Assurance training policy for Defense Cash Accountability System users. The policy should include the training requirements for all Defense Cash Accountability System users, assign monitoring responsibilities, and inform employees of the consequences of not complying with the Information Assurance training policy. Once formalized, they should disseminate the Information Assurance security awareness training policies and procedures to all Defense Cash Accountability System users.**

[22] The application interface requests data from the database to be displayed, added, modified, or deleted. The web server takes the requests, obtains the data from the database, and sends it back to the application interface.

[23] DoD Instruction 8523.01, "Communications Security (COMSEC)," April 22, 2008.

Information and Technology, Defense Finance and Accounting Service Comments

The Director, Information and Technology (I&T), DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that the updated DCAS ACP reflects the IA training requirements. The Director stated that the version update, which was in the process of routing for final signature, requires DCAS users to comply with training requirements to retain access. The Director, I&T, DFAS stated that upon final signature, the updated DCAS ACP will be distributed to all users by October 31, 2016.

Our Response

Comments from the Director partially addressed the recommendation. The updated DCAS ACP, referenced, does not address monitoring responsibilities. For example, the DCAS ACP does not define who is responsible for monitoring and how monitoring is accomplished to ensure all employees complete annual training. In addition, the revised DCAS ACP does not identify the consequences that users will experience if they do not comply with the IA training requirements. For example, the DCAS ACP does not define whether access will immediately be terminated or users will be granted a grace period to complete the training. We request that the Director provide additional comments specifically addressing how and to whom monitoring responsibilities are delegated and managed, and what the consequences are for users who do not comply with the training policy.

b. Review the Defense Cash Accountability System Access Control Policy to determine if it is appropriate for all Center Administrators to be Information System Security Officers. If the policy is appropriate, implement the procedures. If not appropriate, update the policy to identify who should be Information System Security Officers.

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that a review of system roles determined it is appropriate for an ISSO to be appointed as a CA. The DCAS ACP was revised, and final signature is anticipated by October 31, 2016.

Our Response

Comments from the Director partially addressed the recommendation. The updated DCAS ACP, referenced, does not address how this policy will be implemented. For example, the DCAS ACP refers to DCAS CAs as "Center ISSOs." However, the policy does not define when being appointed both CA and ISSO is appropriate and when it is not appropriate. The DCAS ACP does not provide guidance to justify the instances of CAs who were not ISSOs and ISSOs who were not CAs. We request that the Director provide additional comments specifically addressing the actionable plan to implement the dual appointment policy.

c. Develop and implement procedures to:

(1) Require Information System Security Officers to comply with the certification requirements established in DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Program."

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that DFAS is addressing the certification requirements at an organizational level. The Director estimated completion by January 31, 2017.

Our Response

Comments from the Director addressed the specifics of the recommendation, and no further comments are required.

(2) Review the Defense Cash Accountability System service provider's compliance to the terms in the Service Level Agreement. The process should be in accordance with National Institute of Standards and Technology Special Publication 800-35, "Guide to Information Technology Security Services."

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that the DCAS team has reviewed these procedures. As a result, DFAS System Managers are responsible for ensuring compliance with the SLA terms. The Director stated that the DFAS System Manager should provide appropriate information of noncompliance to the DISA Customer Account Representative. The DFAS System Manager provides agreement with the SLA to the DISA Customer Account Representative and maintains responsibility for the applications material within the SLA. DFAS Form 9036, "Request for Agreement Number," must be submitted to the Agency Support Agreements Manager for coordination by DISA when new signatures are required. The Agency Support Agreements Manager coordinates with the Agency Program Management Office to maintain DFAS SLA metrics. The Director stated that these procedures are effective immediately and the action is complete.

Our Response

Comments from the Director addressed the specifics of the recommendation, and no further comments are required.

d. Provide training to applicable Defense Finance and Accounting Service personnel on the Defense Finance and Accounting Service policy to review governance over support and mission work agreements and compliance with Service Level Agreement requirements.

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that the applications DFAS System Manager and the DISA Customer Account Representative review SLAs. At a minimum, SLAs must be signed every 3 years. Any major updates or revisions to the SLA require re-signing the SLA, regardless of when it was last signed. When only minor changes are required, the DFAS System Manager provides agreement to the DISA Customer Account Representative and no new signature is required. The Director stated that the final annual reviewed DISA SLAs are available for reference on the DISA Mission Partner Portal, that these procedures are effective immediately, and that this action is complete.

Our Response

Comments from the Director addressed the specifics of the recommendation, and no further comments are required.

Finding B

Stronger Access Controls Are Needed

Effective application level access controls should be in place to provide reasonable assurance that only authorized personnel have access to the application and only for authorized purposes. DCAS general controls related to access controls were not operating effectively. Specifically:

- DCAS did not automatically log off some users after 15 minutes of inactivity.
- Authorizing officials did not consistently authorize the appropriate access for DCAS users.
- DCAS CAs did not conduct periodic reviews to assess the continued appropriateness of DCAS user access roles, including roles with access to sensitive transactions and activities.
- BEIS Office personnel did not ensure that DCAS always generated exception reports.

This occurred because BEIS Office personnel responsible for DCAS did not regularly follow the DISA Security Technical Implementation Guide (STIG)[24] and policies defined in the ACP. As a result, users may have unauthorized access to DCAS. Without effective application access controls, individuals may obtain unauthorized or inappropriate access to DCAS and its information.

Automatic Logout Exceptions Were Not Justified

DCAS did not automatically log off some users after 15 minutes of inactivity. The DISA STIG requires any continuous inactive period during a user's session (idle time) to be either limited to 15 minutes or authorized and documented. DCAS had seven user profiles that established a group of privileges and system settings. Of the seven DCAS profiles, six profiles automatically logged off users after 15 minutes of inactivity. Only one profile allowed unlimited idle time necessary for long-running queries and other operations.

DCAS Information Assurance Officer (IAO) Support personnel used an approved System Authorization Access Request (SAAR)[25] to create user access and assign the

[24] Security Technical Implementation Guide (STIG), "Oracle 11g Database STIG – Version 8, Release 1.13 Instance Manual," April 24, 2015.

[25] In addition to maintaining SAARs, IAO Support personnel also create user accounts and manage access.

appropriate profile to each of the eight production support users reviewed. The ACP requires authorizing officials[26] to review the users' SAARs for completeness, ensuring all eligibility prerequisites[27] are met.

Eight production support users were assigned to the user profile with unlimited idle time. However, the users' supervisors and DCAS Information Owners (IOs)[28] or their representatives did not justify on the SAARs why the eight production support users required unlimited idle privilege. For example, six SAARs simply stated, "Access needed for production support of the DCAS application." The remaining two SAARs said that the users were developers who required the rights to the DCAS version control repositories without further explanation. Without the documented evidence of need as required by the DISA STIG, the BEIS Office did not have assurance that the eight users indeed required unlimited access privileges.

This occurred because the various authorizing officials did not adequately perform their reviews to ensure the production support users met the eligibility prerequisites. Although a supervisor approved all eight SAARs, the next-level authorizing officials did not sign any of the SAARs. Without the IOs (or their representatives) and the IAOs approving the access requests as required, the benefits of multi-level reviews and approvals were bypassed. For example, the next-level review should have identified that the security managers did not validate security clearance or background investigations for three of the eight SAARs. Consequently, the DCAS IAO Support personnel applied the profile with unlimited idle time privileges to the production support users' access without properly approved SAARs.

As a result, these users may have been assigned to a profile with unlimited access privileges and therefore accessed DCAS inappropriately. Moreover, without justification for unlimited idle time, anyone (including passersby) could view or access data when they do not have a need-to-know. BEIS Office management should develop and document procedures to identify those users, including production support users, who are approved to have the unlimited idle time profile and the documentation to support the request.

Without justification for unlimited idle time, anyone...could view or access data when they do not have a need-to-know.

[26] Individuals requesting user access complete the SAAR and submit the SAAR to authorizing officials, including senior managers. "Authorizing officials" refers to all the levels of validation required in the process: supervisor, security manager, IO, IAO, and DCAS IAO Support Office personnel.

[27] Eligibility prerequisites include security clearance or background investigations, access approval, need-to-know determination, interconnection controls, and IA training.

[28] The DCAS IOs or their representatives must adequately indicate on the SAAR the roles and organizations for which access is required. If the user requires differing access profiles for different organizations or centers, the IOs or their representatives must explain this on the SAAR.

Level of Access Inconsistently Authorized

Authorizing officials did not consistently authorize the appropriate access to DCAS users. The ACP states that all DCAS data is sensitive, and therefore requires all users to meet certain eligibility prerequisites, including a valid business need. The ACP also states that certain DCAS user roles have the ability to perform three sensitive activities:

- grant new users access or roles;
- update, modify, or delete transactions; and
- validate or update source data tables.

The ACP requires each next-level authorizing official to review a user's SAAR for completeness to ensure that the appropriate access levels and unique controls are granted based on the user's roles. Authorizing officials must document their review on the SAAR and provide the SAAR to the DCAS IAO Support Office. DCAS IAO Support Office personnel will then create the user's account in DCAS based on the access requested on the approved SAAR.

We randomly selected 78 DCAS users from a list of all users provided by DFAS and obtained each user's SAAR. Of the 78 users, 56 DCAS users had access to sensitive activities. The supervisors, ISSOs, and IOs or their representatives did not sign 2 of the 56 SAARs. Both users had unauthorized access to sensitive financial activities and could modify financial data or transactions in DCAS. The authorizing officials did not sign the SAARs to ensure that these two users completed eligibility prerequisites as required. Even though the authorizing officials did not sign the SAARs, DCAS IAO Support Office personnel granted the two users access to perform sensitive activities in DCAS. Using the control test outlined in section 450, table I, Government Accountability Office (GAO) Financial Audit Manual, if more than one control exception occurs, then the control is deemed ineffective. Therefore, the system was at risk of unauthorized user access because the control was not fully operating as designed.

This occurred because the authorizing officials did not follow the ACP for reviewing, documenting, and approving the SAARs. When asked, the authorizing officials could not explain why they did not follow the ACP when granting access to users. As a result, authorizing officials increased the risk of granting ineligible individuals the ability to perform sensitive activities in DCAS. BEIS Office management should train supervisors, IOs and their representatives, and CAs to validate that each SAAR is complete and requested access levels to perform sensitive

The authorizing officials could not explain why they did not follow the ACP when granting access to users.

activities are appropriate before signing the SAAR and authorizing each user account. Additionally, BEIS Office management should train DCAS IAO Support Office personnel to return incomplete SAARs to the CAs for additional review and completion before creating user accounts and granting access, as required by the ACP.

Periodic Access Permission Reviews Were Not Conducted

The DCAS CAs at each of the four centers[29] did not conduct periodic reviews to assess the continued appropriateness of DCAS user roles including roles with access to sensitive transactions and activities. The ACP requires that CAs conduct three separate reviews of user accounts to ensure only those users with valid business needs gain and maintain access. The ACP also requires CAs to revoke access for terminated or otherwise ineligible users in a timely manner. Specifically, the ACP requires CAs to review:

- monthly reports for terminated users and user accounts with no activity for 45 days;
- user roles for their organizations at least quarterly; and
- user reports quarterly, in coordination with IOs, to ensure a user's access is still valid.

The ACP requires that for each review, the DCAS staff maintain documented evidence of the reviews and any actions taken as a result of that review.

Monthly Reviews of Terminated and Inactive Users Were Not Performed

The DCAS CAs at the four centers did not always review terminated and inactive user reports monthly, as required. The ACP states that the CAs use a monthly report provided by the DCAS Help Desk/Operations Support team (DCAS Help Desk) to identify user accounts with no activity for 45 days. The CAs are required to compare the DCAS Help Desk report to the Human Resources' report (Gains/Losses Report) that shows when employees come into or leave the organization. The CAs should compare the reports and lock user accounts for terminated employees and contact a user's supervisor when there is no activity by the user after 45 days. The user's supervisor must complete and submit a SAAR to the DCAS IAO Support Office as formal documentation of terminated access.

[29] DCAS is administered through four DFAS centers: Cleveland, Indianapolis, Columbus, and Rome.

BEIS Office personnel stated that the DCAS Help Desk personnel were not aware that they were required to prepare the inactivity reports and send them to the CAs. Although two CAs stated that they reviewed the Gains/Losses Report, BEIS Office personnel stated that the CAs did not compare the reports. For instance, the CA for the Cleveland center stated that he had not reviewed the monthly Gains/Losses Reports since October 2014. In addition, the CA for the Columbus center stated that she reviewed the Gains/Losses Reports daily but did not document her reviews. The Columbus CA also confirmed that she did not receive the Gains/Losses Reports and could not identify those users not logging into their accounts after 45 days. BEIS Office personnel stated that they did not have any documentation to provide for the Indianapolis and Rome centers because the respective CAs did not follow the ACP.

DCAS Help Desk personnel were not aware that they were required to prepare the inactivity reports and send them to the CAs.

As a result, DCAS CAs did not always disable or remove inactive accounts and accounts for terminated individuals in a timely manner. By not following standardized ACP procedures, each DCAS Center increased the risk of access to sensitive DCAS data by terminated and otherwise ineligible users. BEIS Office management should provide training to CAs and DCAS Help Desk personnel on their responsibilities and duties to terminate accounts of users who left the organization or had not accessed their account within 45 days, in accordance with the ACP.

Quarterly Reviews of User Roles Were Not Performed

The DCAS CAs did not perform quarterly reviews of the DCAS users to ensure that the roles were still appropriate, as required. According to the ACP, CAs are required to review user roles for their respective organizations at least quarterly. Based on the appropriateness of roles, CAs will document the review and any changes that need to be made and send this information to the DCAS IAO Support Office. DCAS IAO Support Office personnel are required to keep the reports for at least 6 years and 3 months.

According to BEIS Office personnel, the DCAS CAs were not aware that they were required to develop the quarterly reports and send them to the DCAS IAO Support Office for archiving. The BEIS Office personnel provided conflicting explanations for how CAs at the Cleveland center performed the quarterly reviews. For example, a supervisor in the BEIS Office stated that the reviews were not being conducted, while the CA stated that he conducted the reviews but did not send his reports to the DCAS IAO Support Office, to be maintained as required. He said that the reports did not need to be sent to the DCAS IAO Support Office because the quarterly reviews were only required for those users with access to sensitive activities. The Columbus and Indianapolis CAs stated that they did not send support for their quarterly reviews to the DCAS IAO Support Office because they were not aware of the ACP requirement to do so. Officials from the DCAS center in Rome did not respond as to whether they conducted the reviews or not.

As a result, DCAS administrators did not have assurance that user roles were appropriate. By not following the ACP, each DCAS CA increased the risk of access to sensitive DCAS data and activities by unauthorized users. BEIS Office management should train CAs on their responsibilities to review DCAS user roles quarterly, validate that roles remain appropriate, document changes, and retain records in accordance with the ACP.

Access to Sensitive Activities Were Not Reviewed Quarterly

While the DCAS CAs at Cleveland consistently conducted reviews to assess the continued appropriateness of users' access to sensitive DCAS activities, the CAs at the Columbus, Indianapolis, and Rome centers did not. The ACP states that the DCAS Help Desk will send a list of all users with access to sensitive activities to the CAs for a 100-percent review on a quarterly basis. The ACP also requires CAs to lock any user account when their review determines that the user no longer needs access to sensitive activities in DCAS. In addition, the ACP states that the CAs will work with the users and the users' supervisors to update DCAS access with updated SAARs.

The CAs at the Columbus, Indianapolis, and Rome centers stated that they conducted the quarterly reviews of the user roles; however, the documentation was incomplete or did not support that reviews were conducted. For instance, the Columbus CA provided documentation that did not include the actions taken as a result of her review, to include whether she locked users' accounts because the users no longer required access to sensitive activities. The Indianapolis CA also provided incomplete, and in some instances inaccurate, documentation. For example, the supervisor's contact information on the documentation for five users was not current, yet those supervisors were asked to validate the users' continued need for access. Also, we found two instances when the supervisors relied on the users to validate that they still required access to sensitive activities. Lastly, the Rome CA provided documentation that did not contain any evidence that she conducted quarterly reviews.

This occurred because the CAs did not follow the procedures outlined in the ACP to conduct quarterly reviews of DCAS users with access to sensitive activities and ensure each user still required this level of access in the system. When asked, the CAs could not explain why they did not follow the ACP. As a result, terminated and otherwise ineligible users may have continued to access DCAS, increasing the risk of unauthorized access to sensitive data and activities. Without proper, regular, and supported reviews, DCAS system owners did not have assurance that user roles were appropriate and the information in DCAS remained secure. BEIS Office management should train supervisors and DCAS CAs on their responsibilities to conduct quarterly 100-percent reviews of users' access to sensitive DCAS activities for continued appropriateness, and the CAs' duties to lock any user's account that is no longer appropriate, in accordance with the ACP.

Controls for Multiple Logins Were Inconsistent

BEIS Office personnel did not ensure that DCAS always generated reports (exception reports) showing a user's login and logout activity for the previous day. Specifically, the DCAS System Security Officer did not review the exception reports to validate that user logins were appropriate or whether users having more than two active sessions at the same time (multiple logins) were valid. The ACP states that BEIS Office personnel should use system-generated reports to monitor DCAS activity for potential security violations. The reports identify excessive login attempts, multiple logins, and daily login and logout activity by DCAS users. DCAS systematically e-mailed the exception reports to the DCAS System Security Officer for review. In addition, the ACP requires that any potential security events be reviewed, and, if suspicious activity is identified, the DCAS System Security Officer will escalate the activity to a higher level. The ACP also requires the DCAS ISSO to resolve any ACP procedure that is violated.

However, DCAS did not always generate the user exception reports for the previous day's activity, as required. For example, while DFAS performed system maintenance on DCAS in January 2015, the system did not generate the reports for 2 days while system maintenance was performed. In another example, DCAS did not generate the exception reports for a period of 7 days, March 25-31, 2015 for the last 7 days of the FY 2015 second reporting quarter. BEIS Office personnel stated that they did not know why the system stopped preparing the reports. Lastly, a DCAS exception report dated for December 31, 2014, showed that three DCAS users each had multiple logins that should have been investigated; however, BEIS Office personnel did not provide records to show whether a review of the activity had been conducted.

BEIS Office personnel stated that they did not know why the system stopped preparing the reports.

The DCAS System Security Officers are also required to document their reviews of exceptions reports and any actions taken. However, the DCAS System Security Officer did not document why DCAS stopped preparing exception reports during system maintenance or for 7 days at the end of the FY 2015 second reporting quarter. In addition, BEIS Office personnel could not explain who was notified that DCAS stopped preparing the reports, the actions taken to resolve the problem, and when the reports began generating again.

This occurred because the DCAS System Security Officer did not follow documented procedures outlined in the ACP for consistently reviewing exception reports, taking timely actions when necessary, and documenting the actions taken. In addition, no one monitored DCAS to ensure that exception reports were generated daily. As a result, DCAS had an increased risk of unauthorized access to sensitive data. Without proper, regular, supported reviews, DCAS system owners did not have assurance that users properly accessed DCAS and DCAS data remained secure. BEIS Office management should train DCAS System Security Officers on their responsibilities to review exception reports for potential security violations and escalate any suspicious activity to the DCAS ISSO for resolution, and require DCAS System Security Officers to monitor that DCAS is generating exception reports daily, as required by the ACP.

Recommendations, Management Comments, and Our Response

Recommendation B.1

We recommend that the Director of Business Enterprise Information Services and Other Systems, Defense Finance and Accounting Service:

a. **Develop and document procedures to identify those users, including production support, who are approved to have the unlimited idle time profile and the documentation to support the access request.**

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that the DCAS ACP has been revised to reflect the necessity for the unlimited idle time. DCAS I&T Production Support staff do not have a timeout length to database connections based on inactivity because their positions are to provide support and problem solving. The Director stated that upon final signature, the updated DCAS ACP will be distributed to all users by October 31, 2016.

Our Response

Comments from the Director addressed the specifics of the recommendation, and no further comments are required.

b. Train supervisors, Information Owners and their representatives, and Center Administrators to validate that each System Authorization Access Request is complete and requested access levels to perform sensitive activities are appropriate before signing the System Authorization Access Request and authorizing each user account.

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that the DCAS ACP has been revised with a more detailed procedure to consistently and accurately process SAAR forms. DCAS CAs should review requests for accuracy before signing for the requested access level to perform sensitive activities. Additionally, the DCAS ACP revision includes an added appendix that shows where approvers should sign the SAAR and the routing order. Upon final signature, the updated DCAS ACP will be distributed to all users by October 31, 2016. The Director stated that all 'New User' and 'Modification' access requests will be processed in an automated Account Management and Provisioning System (AMPS) beginning October 21, 2016.

Our Response

Comments from the Director addressed the specifics of the recommendation, and no further comments are required.

c. Train Defense Cash Accountability System Information Assurance Officer Support Office personnel to return incomplete System Authorization Access Requests to the Center Administrators for additional review and completion before creating user accounts and granting access, in accordance with the Access Control Policy.

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that the appropriate Information System Security Office personnel have been trained and are now properly reviewing SAARs in accordance with the DCAS ACP. The Director stated that all 'New User' and 'Modification' access requests will be processed in AMPS beginning October 21, 2016. Incomplete requests in AMPS can be rejected, and revalidation requests will automatically be sent back to the users for more information. The Director stated that the action is complete.

Our Response

Comments from the Director addressed the specifics of the recommendation, and no further comments are required.

d. Train Center Administrators and Defense Cash Accountability System Help Desk personnel on their responsibilities and duties to terminate accounts of users who left the organization or had not accessed their accounts within 45 days.

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that a system change request was implemented on October 15, 2013. As a result of the automated functionality and logic inserted into DCAS by the system change request, DCAS will send warnings to users at the 15-day mark to log into the system by the given date or their accounts will be locked. At the 30-day mark, DCAS will automatically lock the accounts. The Director stated that the action is complete.

Our Response

Comments from the Director partially addressed the recommendation. The Director did not address plans to train DCAS CAs and Help Desk personnel on their responsibilities and duties relating to users who have left the organization. Although the functionality and logic of DCAS allows for automated operations, such as locking accounts with 30 days of inactivity, CAs and Help Desk personnel should not rely on DCAS to ensure that the accounts of users who have left the organization are terminated. Therefore, we ask that the Director provide additional comments specifically addressing the actionable plan to train personnel on their responsibilities and duties to terminate accounts of separated users.

e. Train Center Administrators on their responsibilities to review Defense Cash Accountability System user roles quarterly, validate that roles remain appropriate, document changes, and retain records in accordance with the Access Control Policy.

Information and Technology, Defense Finance and Accounting Service Comments

The Director I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that CAs were reminded of their responsibilities during a summit meeting on March 23, 2016. Specifically, CAs should follow the DCAS ACP and review DCAS user roles quarterly, validate the appropriateness of user roles, document changes, and retain records. The Director stated that the action is complete.

Our Response

Comments from the Director addressed the specifics of the recommendation, and no further comments are required.

f. Train supervisors and Center Administrators on their responsibilities to conduct quarterly 100-percent reviews of users' access to sensitive Defense Cash Accountability System activities for continued appropriateness, and the Center Administrators' duties to lock any user's account that is no longer appropriate, in accordance with the Access Control Policy.

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that CAs were reminded of their responsibilities during a summit meeting on March 23, 2016. Specifically, CAs should follow the DCAS ACP and conduct quarterly 100-percent reviews of users' access to sensitive DCAS activities for continued appropriateness. The Director stated that this action is complete.

Our Response

Comments from the Director addressed the specifics of the recommendation, and no further comments are required.

g. Train Defense Cash Accountability System Security Officers on their responsibilities to review exception reports for potential security violations and escalate any suspicious activity to the Defense Cash Accountability System Information System Security Officer for resolution, and require System Security Officers to monitor that Defense Cash Accountability System is generating exception reports daily, as required by the Access Control Policy.

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that DCAS System Administration team began reviewing and approving exception reports for potential security violations. On November 12, 2015, the system manager signed the Access Audit Log Tracking Procedure, and the DCAS Security Officer was subsequently trained. The DCAS Security Officer began conducting the reviews, monitoring the reports, and escalating suspicious activity in accordance with the revised DCAS ACP. The Director stated that upon final signature, the updated DCAS ACP will be distributed to users by October 31, 2016.

Our Response

Comments from the Director addressed the specifics of the recommendation, and no further comments are required.

Finding C

Information System Contingency Plan Not Coordinated or Updated

Contingency planning is designed to mitigate the risk of system and service unavailability by providing effective and efficient solutions to enhance system availability. The DCAS general controls related to contingency planning were not operating effectively. Specifically, the BEIS Office did not:

- Coordinate the DCAS Information System Contingency Plan (the contingency plan) with the organizational offices responsible for supporting plans, such as the Business Continuity, Disaster Recovery, and Continuity of Operation Plans. This occurred because BEIS Office personnel believed that they were not required to comply with the NIST requirement for contingency planning until 2017. As a result, DFAS did not have assurance that DCAS was a priority for recovery during an organization-wide disaster.
- Update or revise the contingency plan and related agreements to correct deficiencies identified during internal contingency plan testing. This occurred because BEIS Office personnel acquired responsibility of DCAS from DLA but did not ensure that deficiencies were addressed and the plan was updated prior to transition. As a result, DFAS may not be able to use DCAS in the event of a disaster.

Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an entity's ability to accomplish its mission. If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information.

Contingency Plan Not Coordinated With Key Organizations

DFAS did not coordinate the contingency plan with other organizational offices responsible for supporting plans or update the contingency plan after testing to ensure that recovery strategies and supporting resources were not duplicated or negated. According to NIST,[30] the contingency plan represents a broad scope of activities designed to sustain and recover critical system services following an

[30] NIST Special Publication 800-34 Rev. 1 "Contingency Planning Guide for Federal Information Systems," May 2010, updated November 2010.

emergency event. Information system contingency planning fits into a much broader security and emergency management effort that includes organizational and business process continuity, disaster recovery planning, and incident management. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's information systems, mission/business processes, personnel, and the facility. Because there is an inherent relationship between an information system, the mission, and the business process it supports, there must be coordination between each plan during development. Additionally, the plan should be updated to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

According to NIST, the Contingency Plan Coordinator should evaluate supporting plans to ensure that the information is current and continues to meet system requirements adequately. Additionally, NIST requires the organization coordinate contingency plan development with organizational elements responsible for related plans[31] to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

BEIS Office personnel stated that they did not coordinate the DCAS contingency plan with the other organizational elements because they were following a timeline in an Information Paper (memorandum) issued by the DoD Chief Information Officer[32] to transition from the DoD Information Assurance Certification and Accreditation Process to the Risk Management Framework. The memorandum stated that for systems with DoD Information Assurance Certification and Accreditation Process packages submitted through May 31, 2015, those system owners did not need to change or update their package to meet the Risk Management Framework requirements until 2½ years from the authorizing official signature date. The authorizing official signature date for the DCAS package was July 9, 2014. However, the NIST requirement was in place since November 2010, 4 years before the DoD Chief Information Officer memorandum was issued. Therefore, the contingency plan should have been in place before the DoD Chief Information Officer's memorandum was issued. Without coordination of the contingency plan, DFAS did not have assurance that DCAS was a priority for recovery during an organization-wide disaster. The BEIS Office management should implement processes to coordinate the contingency plan with the organizational

[31] Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

[32] DoD issued an Information Paper (memorandum) on September 19, 2014, to provide information on the revised timeline from the DoD Information Assurance Certification and Accreditation Process (DIACAP) to the Risk Management Framework (RMF), found within DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology (IT)," March 12, 2014.

offices responsible for the Business Continuity, Disaster Recovery, and Continuity of Operation Plans. Based on the information received from the organizational offices, BEIS Office management should update the DCAS contingency plan accordingly.

Information Security Contingency Plan Not Updated

The BEIS Office did not update and revise the contingency plan, as well as the Business Continuity Plans, Disaster Recovery Plans, and Crisis Communications Plans to correct the deficiencies identified during testing of the contingency plan. NIST[33] requires that the plan coordinator update the contingency plan, if appropriate, by implementing recommendations made in the after action report. Contingency test results provide an important measure of the feasibility of the plan. Any testing of the plan is likely to identify weaknesses, and it is important that the plan and related supporting activities, such as training, be revised to address these weaknesses. The benefits of the testing are to identify and correct weaknesses before the plan needs to be implemented for an actual emergency situation.

In March 2014, DLA prepared an after action report at the conclusion of its contingency plan testing. The report identified four recommendations that required an update to the contingency plan. According to BEIS Office personnel, the contingency plan should have been updated by DLA because DCAS had not transitioned to DFAS at the time the contingency plan was exercised. Regardless of when the contingency plan was exercised, the BEIS Office is now responsible for DCAS and should update the plan accordingly. The last update to the DCAS contingency plan was made in September 2013.

As a result of not completing these updates, DFAS risks not having a contingency plan that will enable it to regain access to DCAS in the event of a disaster. The BEIS Office management should develop and implement processes to ensure recommendations from the contingency plan exercise are incorporated into the contingency plan in a timely manner.

Without completing these updates, DFAS risks not having a contingency plan that will enable it to regain access to DCAS in the event of disaster.

[33] NIST Special Publication 800-84 "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities" dated September 2006, Section 4.5.

Recommendations, Management Comments, and Our Response

Recommendation C.1

We recommend that the Director of Business Enterprise Information Services and Other Systems, Defense Finance and Accounting Service, develop and implement processes to:

a. **Coordinate the Defense Cash Accountability System Information Security Contingency Plan with organizational elements responsible for related plans as required by National Institute of Standards and Technology Special Publication 800-34 Rev. 1 "Contingency Planning Guide for Federal Information Systems," to include Business Continuity, Disaster Recovery, Continuity of Operations, Cyber Incident Response, and Occupant Emergency Plans and update the contingency plan as appropriate.**

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that the DCAS team will not be compliant with NIST until implementing the Risk Management Framework in December 2017. The DCAS team plans to update its Information Security Contingency Plan to include the recommended NIST elements before the December 2017 deadline. The Director estimated completion by January 31, 2017.

Our Response

Comments from the Director partially addressed the recommendation. The Director stated that the DCAS team will not be compliant until December 2017, yet provided an estimated completion date of January 31, 2017. While we normally would not question estimated completion timeframes, we take exception here because of the essence of time for compliance. Therefore, we ask that the Director provide additional comments specifically addressing the estimated completion date, as well as the date necessary to be compliant with NIST.

b. **Incorporate lessons learned from the Information Security Contingency Plan after action report into the Defense Cash Accountability System Information Security Contingency Plan in a timely manner.**

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that the after action report incorporated lessons learned from the 2015 Continuity of Operations Plan, issued timely on March 12, 2015. In 2016, the after action report incorporated lessons learned from the Continuity of Operations plan, also issued timely on February 2, 2016. The Director stated that this action was complete.

Our Response

Comments from the Director partially addressed the recommendation. The Director stated that the after action report incorporated lessons learned from the Continuity of Operations Plan. However, the Director did not provide an action plan to update the DCAS Information Security Contingency Plan based on the after action report. The Information Security Contingency Plan should be updated based on lessons learned from the after action report because testing the plan will identify weaknesses that need to be remediated. DFAS provided the 2015 and 2016 after action reports and exercise plans but not the updated contingency plans. Therefore, we ask that the Director provide additional comments specifically addressing the incorporation of lessons learned from the DCAS Information Security Contingency Plan after action report into the DCAS Information Security Contingency Plan.

Finding D

Configuration Management Controls Need Improvement

Effective configuration management prevents unauthorized changes to DCAS information system resources (for example, software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended. The DCAS general controls related to configuration management were not operating effectively. Specifically:

- BEIS Office personnel did not remove system access for developers no longer working on DCAS. This occurred because BEIS Office personnel did not develop and implement procedures for outgoing or transferring employees to ensure that system accounts were removed in a timely manner as defined by NIST.[34] Without appropriate safeguards, DFAS may have had an increased risk of a developer performing unauthorized changes to the code or modifying the DCAS application functionality.
- BEIS Office personnel could not verify or track that authorized system changes were made to the DCAS production environment.[35] In addition, BEIS Office personnel had no way to validate that only approved changes were implemented. This occurred because BEIS Office personnel did not have policies and procedures to identify, track, and verify all changes made to the DCAS production environment were approved. As a result, BEIS Office personnel could not ensure that authorized changes were implemented and that there were no unauthorized changes or malicious code[36] placed into the production environment that could affect the functionality of the system.
- BEIS Office personnel did not properly define emergency changes.[37] This occurred because BEIS Office personnel were not in compliance with NIST, which requires organizations to include instructions for handling emergency changes within the configuration change control procedures. As a result, BEIS Office personnel may not be able to implement an emergency change to prevent significant functionality problems, critical information could become inaccurate, or system security could be compromised.

[34] NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook," October 1995.

[35] The application's environment is segregated into system development, testing, and production version (live environment).

[36] Malicious code is software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. For example a virus, worm, or Trojan horse that infects a system.

[37] An emergency change is defined as a critical system discrepancy that prohibits the application or system from running successfully, causes significant errors, affects critical data accuracy, or compromises security.

- BEIS Office personnel responsible for maintaining Master Data Tables[38] did not ensure that changes made by Table Administrators were authorized, configured, and operating securely in DCAS. In addition, Table Administrators did not retain previous versions of the tables in the event they needed to revert back to the prior configuration. This occurred because BEIS Office personnel did not have approved standard operating procedures to properly authorize, test, approve, track, and retain system backups of configuration changes made to the DCAS Master Data Table as required by NIST.[39] As a result, BEIS Office personnel could not ensure that all changes made to the tables were authorized and could not restore to a previous version of the baseline if changes made adversely affected the functionality of the system.
- BEIS personnel did not resolve system vulnerabilities that were identified in DCAS during DISA's vulnerability management scan in October 2014. This occurred because BEIS Office personnel did not have an effective process to identify and address vulnerabilities as defined by NIST.[40] As a result, uncorrected identified vulnerabilities could adversely affect DCAS functionality.

The absence of effective system-level configuration management is a serious risk that jeopardizes an entity's ability to support current and potential requirements. Without effective configuration management, users did not have adequate assurance that DCAS would perform as intended and to the extent needed to support DoD missions.

The Importance of Configuration Management

According to the GAO (FISCAM), an effective configuration management process consists of four primary concepts, each of which should be described in a configuration management plan and implemented according to the plan. They are configuration identification, control, status accounting, and auditing. As part of the configuration control concept, decision makers, such as a configuration control board, evaluate proposed changes on the basis of costs, benefits, and risks, and decide whether to permit a change.

Furthermore, FISCAM states that effective application configuration management consists of configuration management controls to ensure that only authorized changes are made to the system. These controls provide reasonable assurance

[38] Master data is application, non-privileged, sensitive data such as reference tables, organization tables, crosswalk tables, and report maps.

[39] NIST Special Publication 800-128, "Guide for Security-Focused Configuration Management of Information Systems," August 2011.

[40] NIST Special Publication 800-53 revision 4, "Security and Privacy Controls for Federal Information Systems and Organizati5ons" April 2013.

that changes to information system resources are authorized. Configuration management controls are established to ensure that systems are configured and operating securely as intended. In addition, effective application configuration management includes properly authorizing, testing, approving, and tracking all configuration changes.

Entities need to proactively manage the system change environment, application functions, and business processes by restricting and monitoring access to program changes and changes to configurable objects in the production environment. According to the DCAS Configuration Management Plan, the responsibility of managing and performing all configuration management activities within DCAS projects is handled by the DCAS Information and Technology Development team.

System Access for Terminated Developers Was Not Removed in a Timely Manner

Controlling configuration changes includes implementing access restrictions for changes. Access restrictions are a mechanism to enforce configuration control processes by controlling who has access to the information system or its constituent configuration items, or both, to make changes. However, DCAS systems developers[41] no longer working on DCAS still had system access when it should have been removed. According to NIST,[42] a standard set of procedures should be developed to timely remove a user's access for outgoing or transferring employees. The greatest threat to a system is from terminated personnel who maintain access to change code or modify the system or applications. Given the potential for adverse consequences, security specialists routinely recommend that system access be removed as quickly as possible in such situations.

During our review of the developers' access to DCAS in May 2015, the BEIS Office personnel provided a system-generated list of DCAS developers, as well as a BEIS DCAS developer list that contained branch assignments and functional roles. When we compared the two lists, we identified that two developers on the system-generated list were not on the developer branch list. BEIS Office personnel stated the two developers left the agency in February and March 2015.

Based on the initial SAARs received, BEIS Office personnel did not annotate that the access had been removed for the two developers. In May 2015, we requested evidence that the access for the two developers had, in fact, been removed. However, the BEIS Office did not remove the developers' access until after our inquiry.

[41] A systems developer performs all configuration management activities related to technical analysis, design, and source code development within DCAS projects.

[42] NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook," October 1995.

BEIS Office personnel did not remove system access in a timely manner because they did not have any procedures for removing developer access as required by NIST. Specifically, BEIS Office personnel did not have procedures that defined the roles and responsibilities for removing developer access or the timeframes for completing the action. Without appropriate safeguards, DFAS has an increased risk of a developer performing unauthorized changes to the code or modifying the DCAS application functionality. BEIS Office management should develop and implement employee outprocessing procedures to ensure access for terminated developers is removed in a timely manner and document the removal of access on the SAAR.

Without appropriate safeguards, DFAS has an increased risk of a developer performing unauthorized changes to the code or modifying the DCAS application functionality.

Production Changes Were Not Verified or Tracked

BEIS Office personnel did not verify or track that changes made to the production environment[43] of DCAS were authorized. In addition, the BEIS Office personnel could not validate that only approved system changes were implemented. According to NIST,[44] configuration change control is the process to ensure that configuration changes to an information system are formally requested, evaluated for their security impact, tested for effectiveness, and approved before they are implemented. Although the process may have different steps and levels of rigor, one step is to verify that the change was implemented correctly. Configuration change control is not complete and a change request is not closed until confirmation that the change was deployed without problems.

The BEIS Office personnel performed three procedures to verify that tested and approved configuration changes were implemented into the production environment. These procedures were defined as "audits" in the DCAS Configuration Management Plan. However, these procedures did not ensure that all configuration items[45] approved for release into production were actually implemented. The three procedures performed are described below.

- Physical Configuration Audits: designed to identify all configuration items associated with changes that were developed, tested, and approved for release into the production environment.

[43] The application's environment is divided into three areas: system development, testing, and production.

[44] NIST Special Publication 800-128, "Guide for Security-Focused Configuration Management of Information Systems," August 2011.

[45] Configuration Items are a set of elements that comprise a DCAS source code.

- Database and Application Server Implementation Audits: designed to compare the DCAS production environment before and after configuration changes were implemented to the system, and ensure that the production baseline (or environment) was not modified in an unauthorized manner.
- Internal Release Audits: served as a monitoring mechanism to ensure that only authorized changes were made to the DCAS production environment over the course of the prior calendar month.

Our review of the Physical Configuration Audits compared to the Database and Application Server Implementation Audits demonstrated that not all configuration changes were tracked. BEIS Office personnel stated that not all configuration items would be identified in the Database and Application Server Implementation Audits as these audits were not designed to track these items. As a result, not all configuration items identified in the Physical Configuration Audits were tracked in the Database and Application Server Implementation Audits. Therefore, these procedures (audits) did not verify that approved changes were released into production.

In addition, our review of the provided Internal Release Audits documentation showed that each release package had the necessary related documentation. However, it did not demonstrate that the DCAS System Manager or the Audit Readiness Lead verified and validated that only authorized changes were made in production as stated in the DCAS Configuration Management Plan.

Overall, our review of these procedures (audits) showed that not all changes made were verified and that changes made in the test environment were not appropriately moved and implemented into the production environment. This occurred because BEIS Office personnel did not have procedures to fully identify, track, and verify that all changes made to the DCAS production environment were approved. As a result, BEIS Office personnel could not ensure that all authorized changes were implemented and no unauthorized changes or malicious code[46] were placed into the production environment that could affect the functionality of the system. BEIS Office management should develop and implement procedures to ensure only authorized changes, including all configuration items, are approved and moved into the DCAS production environment.

[46] Malicious code is software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. For example a virus, worm, or Trojan horse that infects a system.

Emergency Change Procedures Were Undefined

BEIS Office personnel did not properly define emergency changes. According to NIST,[47] unscheduled (emergency) changes may be needed and organizations should include instructions for handling emergency changes within the configuration change control procedures. The DCAS Configuration Control Board[48] Charter defines an emergency change as a critical system discrepancy that prohibits the application or system from running successfully, causes significant errors, affects critical data accuracy, or compromises security. An emergency change is critical and should be made as soon as possible. Emergency changes are still subject to review by the Configuration Control Board as soon as it is practical after an emergency change is made.

We reviewed five changes that BEIS Office personnel considered emergency changes and found that they did not meet the criteria of an emergency change. Specifically, the five changes were not critical to the functionality of DCAS and did not meet the NIST and the DCAS Configuration Control Board Charter definition of an emergency change. Instead, the System Change Requests identified by BEIS Office personnel were the result of previously identified weaknesses. Based on our analysis, it took between 2 to 4½ months to implement these changes. However, based on the DCAS Configuration Control Board Charter definition of an emergency change, these were not emergency changes because the majority of emergency system change requests are typically accomplished within 24 hours.

BEIS Office personnel did not comply with NIST, which requires policies or procedures to identify emergency changes.

This occurred because the BEIS Office personnel did not comply with NIST, which requires policies or procedures to identify emergency changes, how emergency changes should be handled, and the timeframe to implement emergency changes to ensure minimal impact to of the DCAS functionality. Specifically, the BEIS Office did not develop emergency change procedures in the Configuration Management, Master Software Development, or Testing Management Plans. As a result, BEIS Office personnel may:

- not be able to implement changes to address a critical system discrepancy, which prohibits the application or system from running to a successful completion;

[47] NIST Special Publication 800-128, "Guide for Security-Focused Configuration Management of Information Systems," Section 3.3.2 Unscheduled or Unauthorized Changes, August 2011.

[48] The Configuration Control Board ensures that all functional, legislative, regulatory, security, and technical system change requests are adequately defined and documented prior to consideration for inclusion into a configured release.

- cause significant erroneous functional results;
- affect the accuracy of critical data; or
- compromise system security.

BEIS Office management should develop and implement emergency change policies and procedures to identify emergency changes, including the processes required to fix a critical system discrepancy. The procedures should also include the timeframes for completing the emergency change and clearly distinguish the difference between an emergency and an urgent change.

Incomplete Table Change Documentation

BEIS Office personnel did not ensure that changes made by Table Administrators to the DCAS Master Data Tables[49] were authorized, configured, and operated securely. In addition, BEIS Office personnel did not retain prior versions of the tables in the event they needed to revert back to a previous version of the system's configuration. NIST[50] states that a well-defined configuration change control process is fundamental to any security focused configuration management program. Configuration change control is the process for ensuring that configuration changes to an information system are formally requested, evaluated for their security impact, tested for effectiveness, and approved before they are implemented. NIST also states that if organizations maintain secure configurations for their information systems in an environment where technology is continually evolving and the number and seriousness of threats is expanding, changes to system configurations need to be managed and controlled. As changes are made to baseline configurations, the new baseline becomes the current version, and the previous baseline is no longer valid but is retained for historical purposes. If there are problems with a production release, retention of previous versions allows for a rollback or restoration to a previous secure and functional version of the baseline configuration. Furthermore, NIST states that once the change has been analyzed, approved, tested, implemented, and verified, the organization must ensure that updates have been made to supporting documents to include baseline configurations. Archiving previous baseline configurations is useful for incident response and traceability support during formal audits.

We obtained a list from the BEIS Office personnel of the 23 tables that contained DCAS Master Data Table updates or modifications made by the Table Administrator from October 1, 2014, through March 31, 2015. They also provided the

[49] Master data is application, non-privileged, sensitive data such as reference tables, organization tables, crosswalk tables, and report maps.

[50] NIST Special Publication 800-128, "Guide for Security-Focused Configuration Management of Information Systems," August 2011.

DCAS-generated audit logs to demonstrate when a Table Administrator made a change to a DCAS Master Data Table. DCAS prohibited anyone from modifying a table unless they had a Table Administrator role. However, the table change audit logs did not provide a comprehensive list of all the changes that the Table Administrators made to the DCAS Master Tables. According to the DCAS ACP, there should be an audit log generated by DCAS to show which table was updated, the date and time of the update, the values that were changed, and the identification of the Table Administrator that performed the change. The ACP also requires each Table Administrator to retain documentation supporting the requirement for each table change.

Our review of the DCAS Master Data Table changes showed BEIS Office personnel did not monitor the table changes to ensure that the changes were requested, evaluated for impact to the system, tested for effectiveness, and approved. BEIS Office personnel admitted that not all changes made to a DCAS Master Table could be verified and that they did not monitor the Master Tables for all changes. In addition, BEIS Office personnel did not have an approval process for changes that users could make to their DCAS Master Data Table data before changes took effect as stated in NIST. BEIS Office personnel stated that changes made in the DCAS Master Data Table could not be "rolled back" to a previous table version. In addition, the audit logs were generated solely to meet our request.

BEIS Office personnel admitted that not all changes made to a DCAS Master Table could be verified and that they did not monitor the Master Tables for all changes.

This occurred because DCAS Table Administrators did not have procedures to properly authorize, test, approve, monitor, and track all configuration changes made to the DCAS Master Data Tables. Although the ACP required Table Administrator to retain table change and audit log documentation, the ACP did not address how to store and maintain the documentation. In addition, the audit logs should include all elements defined by the ACP that include which table was updated, the date and time of the update, the values that were changed, and the identification of the Table Administrator that performed the change. As a result, BEIS Office personnel could not ensure that all changes made to the tables were authorized and could not restore to a previous version of the baseline if changes made adversely affected the functionality of the system. BEIS Office management should ensure that the audit logs contain all elements required by the ACP, develop and implement procedures to validate that changes made by Table Administrators to DCAS Master Data Tables are authorized, tested, approved, monitored, and tracked. In addition, the procedures should document how to store and maintain the configuration changes and backups for historical purposes.

Vulnerabilities to Information Systems Were Unresolved

Effective application configuration management includes updating systems in a timely manner to protect against known vulnerabilities. To achieve this goal, entities need to follow an effective process to identify vulnerabilities in applications and update them. NIST[51] states that organizations should:

- perform vulnerability scans[52] on information systems;
- analyze vulnerability scan results; and
- resolve vulnerabilities based on an acceptable level of risk.

DISA runs weekly vulnerability scans and provides application specific vulnerability scan reports to application owners. We requested the vulnerability scan reports from BEIS Office personnel for our period of review; however, BEIS Office personnel stated that they did not start to obtain and maintain the DISA vulnerability scan reports until July 2015. BEIS Office personnel did not address DCAS vulnerabilities that had been identified by DISA from October 2014 through March 2015. Therefore, we did not have assurance that BEIS Office personnel obtained vulnerability scan reports from DISA, analyzed scan results, and resolved vulnerabilities at the time of our review.

This occurred because BEIS Office personnel did not have an effective process that implemented vulnerability identification and addressed vulnerabilities as defined by NIST. As a result, vulnerabilities could adversely affect DCAS functionality if not corrected. BEIS and Other Systems Office management should update the Vulnerability Management plan to clearly define the roles and responsibilities for receipt, analysis of the scans, and appropriate actions needed to resolve system vulnerabilities as required by NIST. In addition, BEIS Office management should train personnel on the roles and responsibilities established in the vulnerability management plan.

Other Matters of Interest

During the audit, we identified a potential lack of independence or segregation of duties[53] over granting and approving developer access. Developers who were part of the configuration management were also responsible for source code changes, including system upgrades and modifications. The manager of the developers

[51] NIST Special Publication 800-53 revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations” April 2013.

[52] Software should be scanned and updated frequently to guard against known vulnerabilities.

[53] According to GAO-14-704G, “Standards for Internal Control in the Federal Government,” September 2014, segregation of duties is defined as where management divides or segregates key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud. Segregation of duties is part of an effective internal control system that helps an entity adapt to shifting environments, evolving demands, changing risks, and new priorities.

approved the SAARs requesting access to DCAS source code. This access was granted by the DCAS Version Control Administrator who reported to this same manager. It is a good business practice to have a specific policy on granting and approving access for developers. Without specific roles identified in policy, this manager could unduly influence the decision to grant access to developers, which could circumvent security.

Recommendations, Management Comments, and Our Response

Recommendation D.1

We recommend that the Director of Business Enterprise Information Services and Other Systems, Defense Finance and Accounting Service:

a. **Develop and implement procedures to:**

   (1) **Remove access for terminated developers in a timely manner and document the removal of access on the System Authorization Access Request form.**

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that the DCAS ACP was revised to address removing access for terminated developers in a timely manner. The Director stated that a removal request will be submitted electronically when AMPS is fully implemented, and AMPS will submit each role awaiting removal to the appropriate de-provisioning process through a remedy ticket. The Director stated that upon final signature, the updated DCAS ACP will be distributed to all users by October 31, 2016.

Our Response

Comments from the Director partially addressed the recommendation. Section 6.4.4.1 of the revised DCAS ACP states, "After one (1) year of inactivity, I&T Development user's account is expired/locked/deactivated. A new SAAR form will be required to re-establish the I&T Development user's access." We do not agree that waiting for 1 year of inactivity meets the intent of the recommendation to remove access in a timely manner. Waiting 1 year allows too much time for unauthorized access to DCAS and potential security threats. Therefore, we request that the Director reconsider the length of time allowed to pass before DCAS automatically deactivates access for inactive I&T Development users and provide additional comments specifically addressing this policy.

(2) Validate that only authorized changes, including all configuration items, are approved and moved to the Defense Cash Accountability System production environment.

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that a system-generated list of all changes within the prior 24-hour period on both database servers was set to run daily in July 2015. An audit log tracking procedure was implemented to require the system management team to review and approve these daily reports for accuracy, completeness, and timeliness. The team member completes a checklist to trace any identified changes back to the configuration items within a release, explaining any anomalies. The review packages are signed and retained. The Director stated that this action is complete.

Our Response

Comments from the Director partially addressed the recommendation. The Director did not address an action plan to ensure all changes made to the DCAS production environment were authorized. In addition, the Director did not address a plan to perform validations to ensure all changes were, in fact, moved into the DCAS production environment. Therefore, we ask that the Director provide additional comments specifically addressing the actionable plans to ensure that only authorized changes, including configuration items, were approved and moved to the DCAS production environment.

(3) Fix a critical system discrepancy (emergency change) that prohibits the application or system from running to a successful completion, causes significant erroneous functional results, affects the accuracy of critical data, or compromises system security. The procedures should include the timeframes for resolving the discrepancy and clearly distinguish between an emergency and urgent change.

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that DCAS team will update the definition of "emergency change" during the annual review of the DCAS Configuration Management and Testing Management Plans. The definition will reflect those of the NIST and DCAS

Configuration Control Board Charter for emergency change and will appropriately address deploying emergency releases. The Director estimated completion by January 31, 2017.

Our Response

Comments from the Director addressed the specifics of the recommendation, and no further comments are required.

(4) Verify changes made by the Table Administrators to the Defense Cash Accountability System Master Data Tables are authorized, tested, approved, monitored and tracked. Additionally, the procedures should document how to store and maintain the configuration changes and backups for historical purposes. In addition, the audit logs should include all elements defined by the ACP that include which table was updated, the date and time of the update, the values that were changed, and the identification of the Table Administrator that performed the change.

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that the DCAS team implemented a release in December 2015 that included a system change request for DCAS master data tables auditability. The DCAS Enterprise Solutions and Standards team created and began using a form in February 2016 to record master data table changes, including which table was updated, the date and time of the update, the values changed, and who made the changes. Audit documentation is stored using Portal Project. The Director stated that this action is complete.

Our Response

Comments from the Director partially addressed the recommendation. We commend the DCAS team for using a standardized form and the portal to ensure all elements relating to DCAS master data table changes are recorded and stored, respectively. However, the Director did not address action plans to ensure the validity, appropriateness, and continued progress and maintenance of DCAS master data tables. Therefore, we ask that the Director provide additional comments specifically addressing the actionable plans to ensure that DCAS master data tables are authorized, tested, approved, monitored, and tracked.

b. Update the Vulnerability Management Plan to ensure the roles and responsibilities are accurately defined for receipt, analysis of the scans, and appropriate actions needed to resolve system vulnerabilities.

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that the DCAS team updated the DCAS Vulnerability Management Plan to include compliance with the DoD IA Vulnerability Management Program in July 2016. Additionally, the DCAS Information System Security Manager and ISSO have a process to review and resolve vulnerabilities identified by the DISA vulnerability management scans. The Information System Security Manager coordinates with the ISSO to record and track the application software vulnerabilities in a system Plan of Action and Milestones report, which is stored on the Enterprise Mission Assurance Support Service website. The Director stated that this action is complete.

Our Response

Comments from the Director addressed the specifics of the recommendation, and no further comments are required.

c. Train applicable BEIS Office personnel on Vulnerability Management Plan responsibilities.

Information and Technology, Defense Finance and Accounting Service Comments

The Director, I&T, DFAS, responding for the Director of BEIS and Other Systems, DFAS, agreed, stating that the applicable DCAS personnel completed training in April 2015 and April 2016 associated with their responsibilities. The Director stated that this action is complete.

Our Response

Comments from the Director addressed the specifics of the recommendation, and no further comments are required.

Appendix

Scope and Methodology

We conducted this FISCAM audit from January 2015 through August 2016 in accordance with generally 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We used the GAO FISCAM, February 2009, to develop the procedures performed during this audit. We limited our audit procedures to the Application Level General Controls as defined by FISCAM.[54] Additionally, we limited our review to first and second quarters FY 2015.

To understand DCAS security management controls, we reviewed the:

- DCAS Security Plan;
- DCAS ACP;
- DCAS DoD Information Assurance Certification and Accreditation Process package;
- Annual IA training certificates;
- ISSO appointment letters;
- ISSO-required certificates;
- DCAS SLA; and
- DISA Statement on Standards for Attestation Engagements 16 report.

To understand DCAS access controls, we reviewed the:

- DCAS ACP;
- DCAS SLA;
- DCAS Security Plan;
- DISA Statement on Standards and Attestation Engagements 16 report;
- SAARs;
- DCAS-generated reports; and
- DCAS system documentation, policies, and procedures.

[54] According to FISCAM, section 4.1, Application Level General Controls consist of general controls operating at the business process application level, including those related to security management, access controls, configuration management, segregation of duties, and contingency planning.

Using the control test outlined in section 450, table I, GAO Financial Audit Manual,[55] we obtained a population of user identifications from DCAS and selected a simple random sample size of 78 out of 7,555 SAARs with a 90-percent confidence level. According to the Manual, if more than one control exception occurs, then the control is deemed ineffective. We requested SAARs for our sample and used the DCAS ACP and the SAAR instructions to ensure that the SAARs were accurately completed and approved.

To understand DCAS contingency plan controls, we reviewed the:

- DCAS Information System Contingency Plan;
- DCAS SLA;
- DISA Services Catalog;
- DCAS tabletop exercise documentation; and
- DCAS after action report.

To understand DCAS configuration management controls, we reviewed the:

- DCAS System Change Requests;
- DCAS Configuration Management Plan;
- DCAS Master Software Development Plan;
- DCAS Testing Management Plan;
- DCAS Master Data Tables;
- DCAS-Generated Audit Logs;
- DCAS ACP;
- system-generated list of DCAS developers;
- BEIS DCAS developer list that contained branch assignments and functional roles;
- SAARs;
- Physical Configuration Audits;
- Database and Application Server Implementation Audits;
- Internal Release Audits;
- DCAS Configuration Control Board Charter; and
- DCAS system documentation, policies, and procedures.

We compared the documentation above to DFAS, DoD, and NIST requirements. In addition, we conducted onsite testing at the DFAS center in Cleveland, Ohio. Furthermore, we interviewed applicable DFAS personnel and followed up on the responses with interviews and documentation requests.

[55] GAO-08-585G, "Financial Audit Manual," Volume 1, July 2008.

Use of Computer-Processed Data

To test the general and application controls within DCAS, we obtained reports from DCAS. We compared these reports to supporting documentation, such as ISSO appointment letters and SAARs, to validate the DCAS information. Based on this comparison and validation of the DCAS reports, we determined that the DCAS information was sufficient to support the findings and conclusions made in the report.

To test DCAS change controls, we also obtained reports from the Configuration Management Information System. We did not test the controls in this system; however, we obtained corroborating evidence to verify information in these reports (see Scope and Methodology). Based on the comparison and validation of the reports, we determined the Configuration Management Information System information was sufficient to support the findings and conclusions made in the report.

Use of Technical Assistance

We received assistance from the Department of Defense Inspector General Quantitative Methods Division to develop our statistical samples of SAARs and System Change Requests.

Prior Coverage

During the last 5 years, GAO and the DoD Inspector General (DoD IG) issued two reports discussing DCAS application level general controls. Unrestricted GAO reports can be accessed at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/pubs/index.cfm.

GAO

Report No. GAO-12-132, "DoD Financial Management: Ongoing Challenges with Reconciling Navy and Marine Corps Fund Balance with Treasury," December 20, 2011

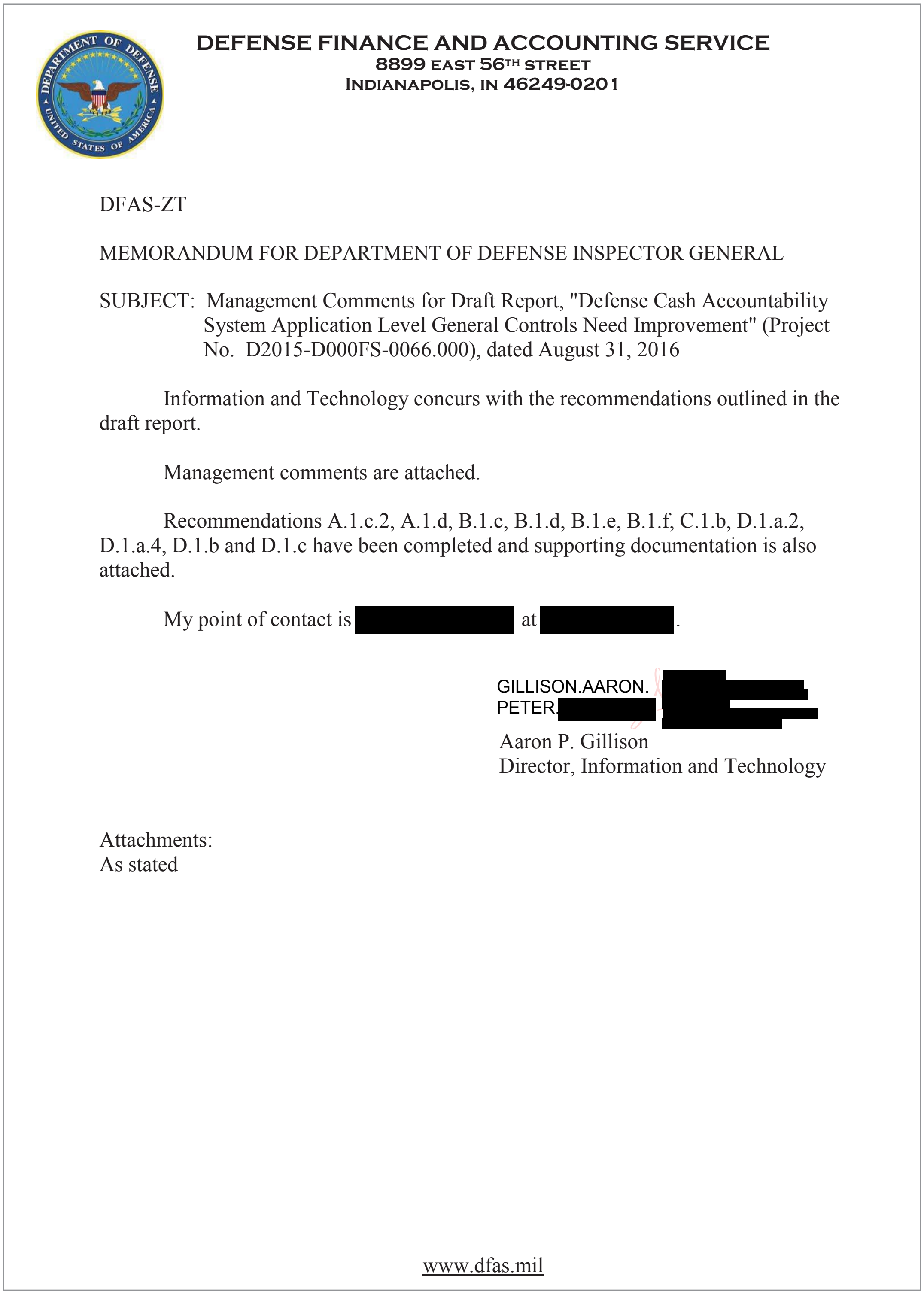
DoD IG

Report No. DODIG-2015-102, "Additional Actions Needed to Effectively Reconcile Navy's Fund Balance With Treasury Account," April 3, 2015

Management Comments

Information and Technology, Defense Finance and Accounting Service

Final Report Reference



DEFENSE FINANCE AND ACCOUNTING SERVICE
8899 EAST 56TH STREET
INDIANAPOLIS, IN 46249-0201

DFAS-ZT

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Management Comments for Draft Report, "Defense Cash Accountability System Application Level General Controls Need Improvement" (Project No. D2015-D000FS-0066.000), dated August 31, 2016

Information and Technology concurs with the recommendations outlined in the draft report.

Management comments are attached.

Recommendations A.1.c.2, A.1.d, B.1.c, B.1.d, B.1.e, B.1.f, C.1.b, D.1.a.2, D.1.a.4, D.1.b and D.1.c have been completed and supporting documentation is also attached.

My point of contact is [redacted] at [redacted].

GILLISON.AARON.
PETER.[redacted] [redacted]

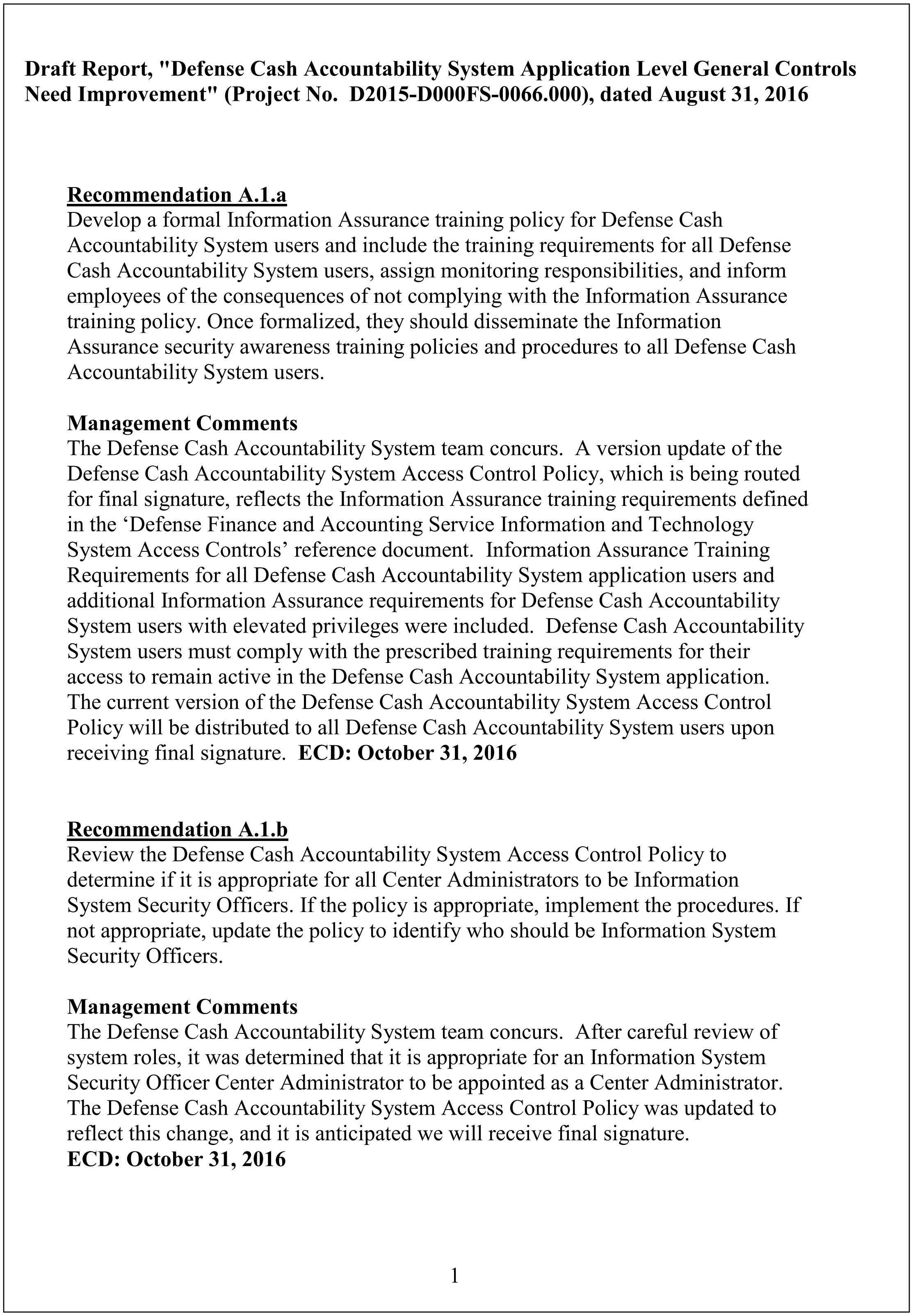
Aaron P. Gillison
Director, Information and Technology

Attachments:
As stated

www.dfas.mil

Supporting documentation provided by Information and Technology, Defense Finance and Accounting Service were omitted because of length. Copies provided upon request.

Information and Technology, Defense Finance and Accounting Service (cont'd)



Draft Report, "Defense Cash Accountability System Application Level General Controls Need Improvement" (Project No. D2015-D000FS-0066.000), dated August 31, 2016

<u>Recommendation A.1.a</u>
Develop a formal Information Assurance training policy for Defense Cash Accountability System users and include the training requirements for all Defense Cash Accountability System users, assign monitoring responsibilities, and inform employees of the consequences of not complying with the Information Assurance training policy. Once formalized, they should disseminate the Information Assurance security awareness training policies and procedures to all Defense Cash Accountability System users.

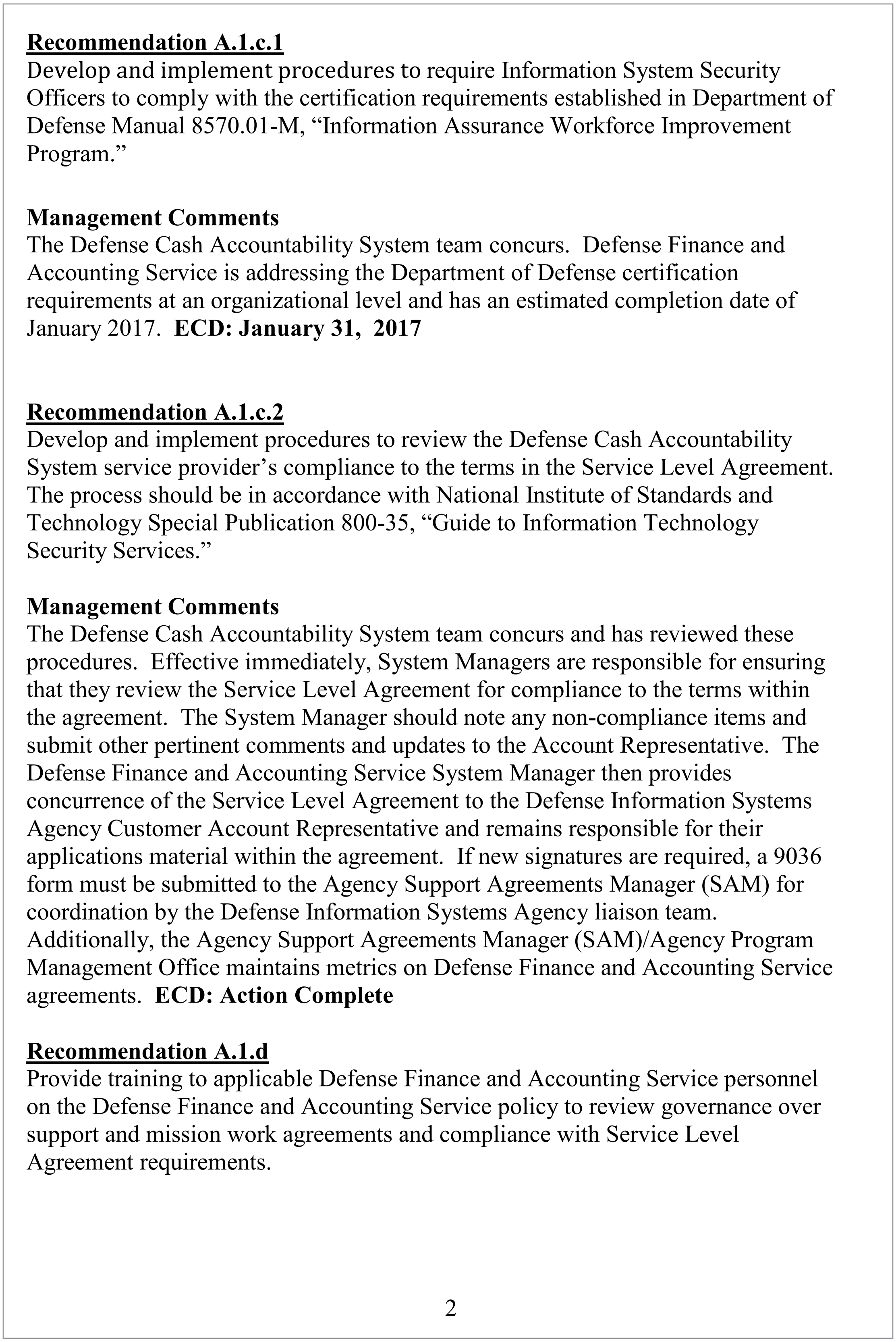
Management Comments
The Defense Cash Accountability System team concurs. A version update of the Defense Cash Accountability System Access Control Policy, which is being routed for final signature, reflects the Information Assurance training requirements defined in the 'Defense Finance and Accounting Service Information and Technology System Access Controls' reference document. Information Assurance Training Requirements for all Defense Cash Accountability System application users and additional Information Assurance requirements for Defense Cash Accountability System users with elevated privileges were included. Defense Cash Accountability System users must comply with the prescribed training requirements for their access to remain active in the Defense Cash Accountability System application. The current version of the Defense Cash Accountability System Access Control Policy will be distributed to all Defense Cash Accountability System users upon receiving final signature. **ECD: October 31, 2016**

<u>Recommendation A.1.b</u>
Review the Defense Cash Accountability System Access Control Policy to determine if it is appropriate for all Center Administrators to be Information System Security Officers. If the policy is appropriate, implement the procedures. If not appropriate, update the policy to identify who should be Information System Security Officers.

Management Comments
The Defense Cash Accountability System team concurs. After careful review of system roles, it was determined that it is appropriate for an Information System Security Officer Center Administrator to be appointed as a Center Administrator. The Defense Cash Accountability System Access Control Policy was updated to reflect this change, and it is anticipated we will receive final signature.
ECD: October 31, 2016

1

Information and Technology, Defense Finance and Accounting Service (cont'd)



Recommendation A.1.c.1

Develop and implement procedures to require Information System Security Officers to comply with the certification requirements established in Department of Defense Manual 8570.01-M, "Information Assurance Workforce Improvement Program."

Management Comments

The Defense Cash Accountability System team concurs. Defense Finance and Accounting Service is addressing the Department of Defense certification requirements at an organizational level and has an estimated completion date of January 2017. **ECD: January 31, 2017**

Recommendation A.1.c.2

Develop and implement procedures to review the Defense Cash Accountability System service provider's compliance to the terms in the Service Level Agreement. The process should be in accordance with National Institute of Standards and Technology Special Publication 800-35, "Guide to Information Technology Security Services."

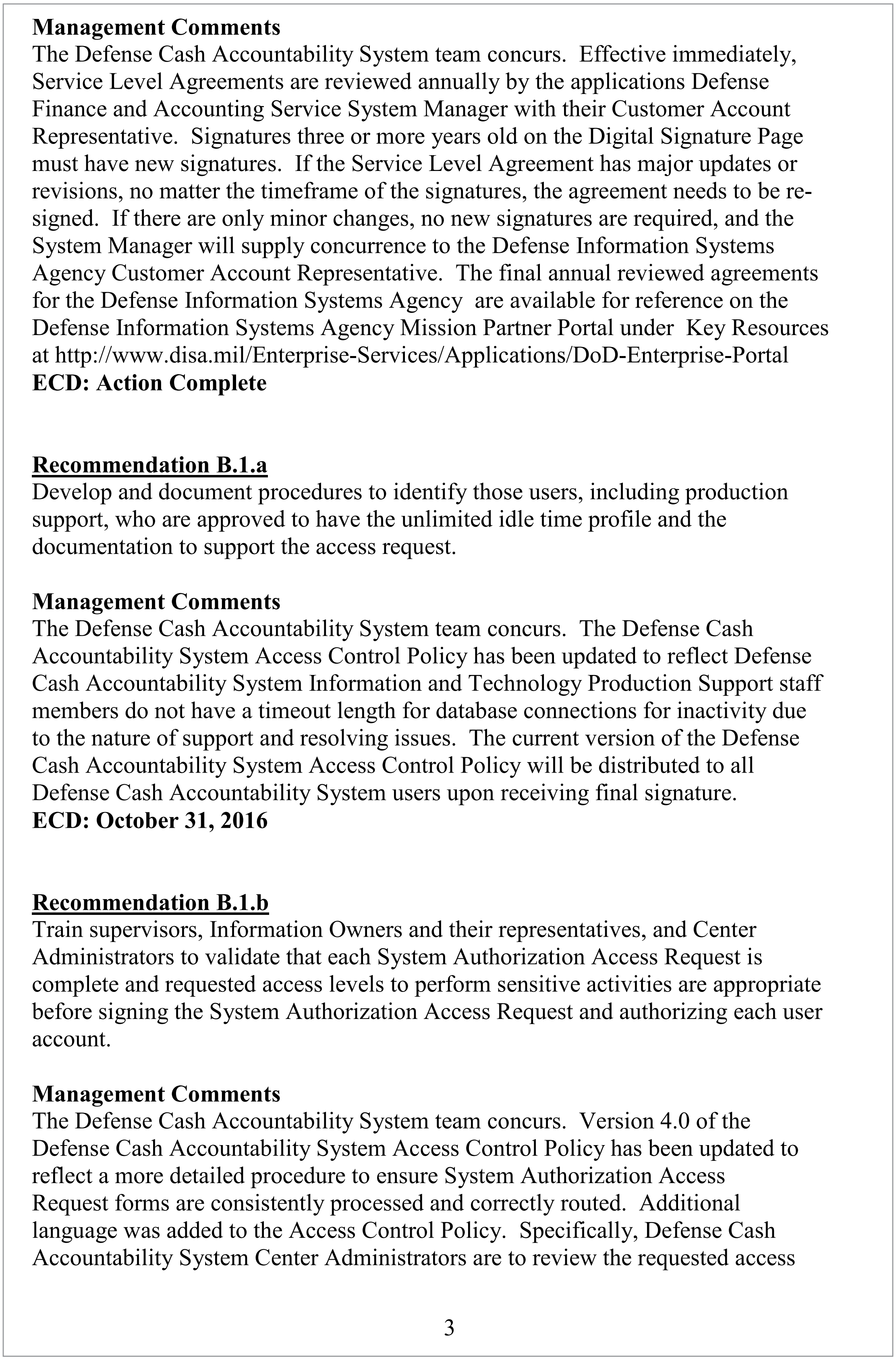
Management Comments

The Defense Cash Accountability System team concurs and has reviewed these procedures. Effective immediately, System Managers are responsible for ensuring that they review the Service Level Agreement for compliance to the terms within the agreement. The System Manager should note any non-compliance items and submit other pertinent comments and updates to the Account Representative. The Defense Finance and Accounting Service System Manager then provides concurrence of the Service Level Agreement to the Defense Information Systems Agency Customer Account Representative and remains responsible for their applications material within the agreement. If new signatures are required, a 9036 form must be submitted to the Agency Support Agreements Manager (SAM) for coordination by the Defense Information Systems Agency liaison team. Additionally, the Agency Support Agreements Manager (SAM)/Agency Program Management Office maintains metrics on Defense Finance and Accounting Service agreements. **ECD: Action Complete**

Recommendation A.1.d

Provide training to applicable Defense Finance and Accounting Service personnel on the Defense Finance and Accounting Service policy to review governance over support and mission work agreements and compliance with Service Level Agreement requirements.

Information and Technology, Defense Finance and Accounting Service (cont'd)



Management Comments
The Defense Cash Accountability System team concurs. Effective immediately, Service Level Agreements are reviewed annually by the applications Defense Finance and Accounting Service System Manager with their Customer Account Representative. Signatures three or more years old on the Digital Signature Page must have new signatures. If the Service Level Agreement has major updates or revisions, no matter the timeframe of the signatures, the agreement needs to be re-signed. If there are only minor changes, no new signatures are required, and the System Manager will supply concurrence to the Defense Information Systems Agency Customer Account Representative. The final annual reviewed agreements for the Defense Information Systems Agency are available for reference on the Defense Information Systems Agency Mission Partner Portal under Key Resources at http://www.disa.mil/Enterprise-Services/Applications/DoD-Enterprise-Portal
ECD: Action Complete

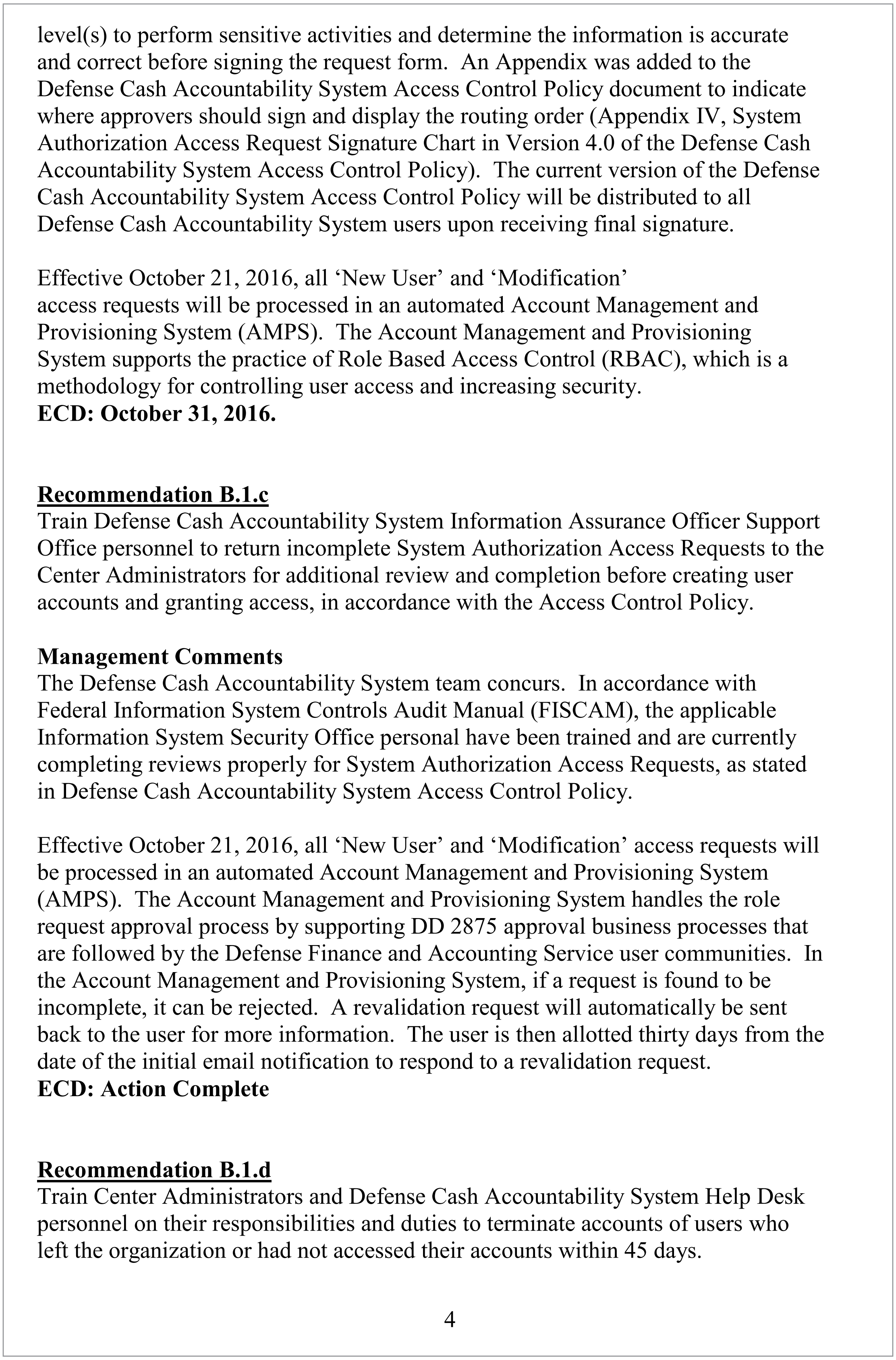
Recommendation B.1.a
Develop and document procedures to identify those users, including production support, who are approved to have the unlimited idle time profile and the documentation to support the access request.

Management Comments
The Defense Cash Accountability System team concurs. The Defense Cash Accountability System Access Control Policy has been updated to reflect Defense Cash Accountability System Information and Technology Production Support staff members do not have a timeout length for database connections for inactivity due to the nature of support and resolving issues. The current version of the Defense Cash Accountability System Access Control Policy will be distributed to all Defense Cash Accountability System users upon receiving final signature.
ECD: October 31, 2016

Recommendation B.1.b
Train supervisors, Information Owners and their representatives, and Center Administrators to validate that each System Authorization Access Request is complete and requested access levels to perform sensitive activities are appropriate before signing the System Authorization Access Request and authorizing each user account.

Management Comments
The Defense Cash Accountability System team concurs. Version 4.0 of the Defense Cash Accountability System Access Control Policy has been updated to reflect a more detailed procedure to ensure System Authorization Access Request forms are consistently processed and correctly routed. Additional language was added to the Access Control Policy. Specifically, Defense Cash Accountability System Center Administrators are to review the requested access

Information and Technology, Defense Finance and Accounting Service (cont'd)



level(s) to perform sensitive activities and determine the information is accurate and correct before signing the request form. An Appendix was added to the Defense Cash Accountability System Access Control Policy document to indicate where approvers should sign and display the routing order (Appendix IV, System Authorization Access Request Signature Chart in Version 4.0 of the Defense Cash Accountability System Access Control Policy). The current version of the Defense Cash Accountability System Access Control Policy will be distributed to all Defense Cash Accountability System users upon receiving final signature.

Effective October 21, 2016, all 'New User' and 'Modification' access requests will be processed in an automated Account Management and Provisioning System (AMPS). The Account Management and Provisioning System supports the practice of Role Based Access Control (RBAC), which is a methodology for controlling user access and increasing security.
ECD: October 31, 2016.

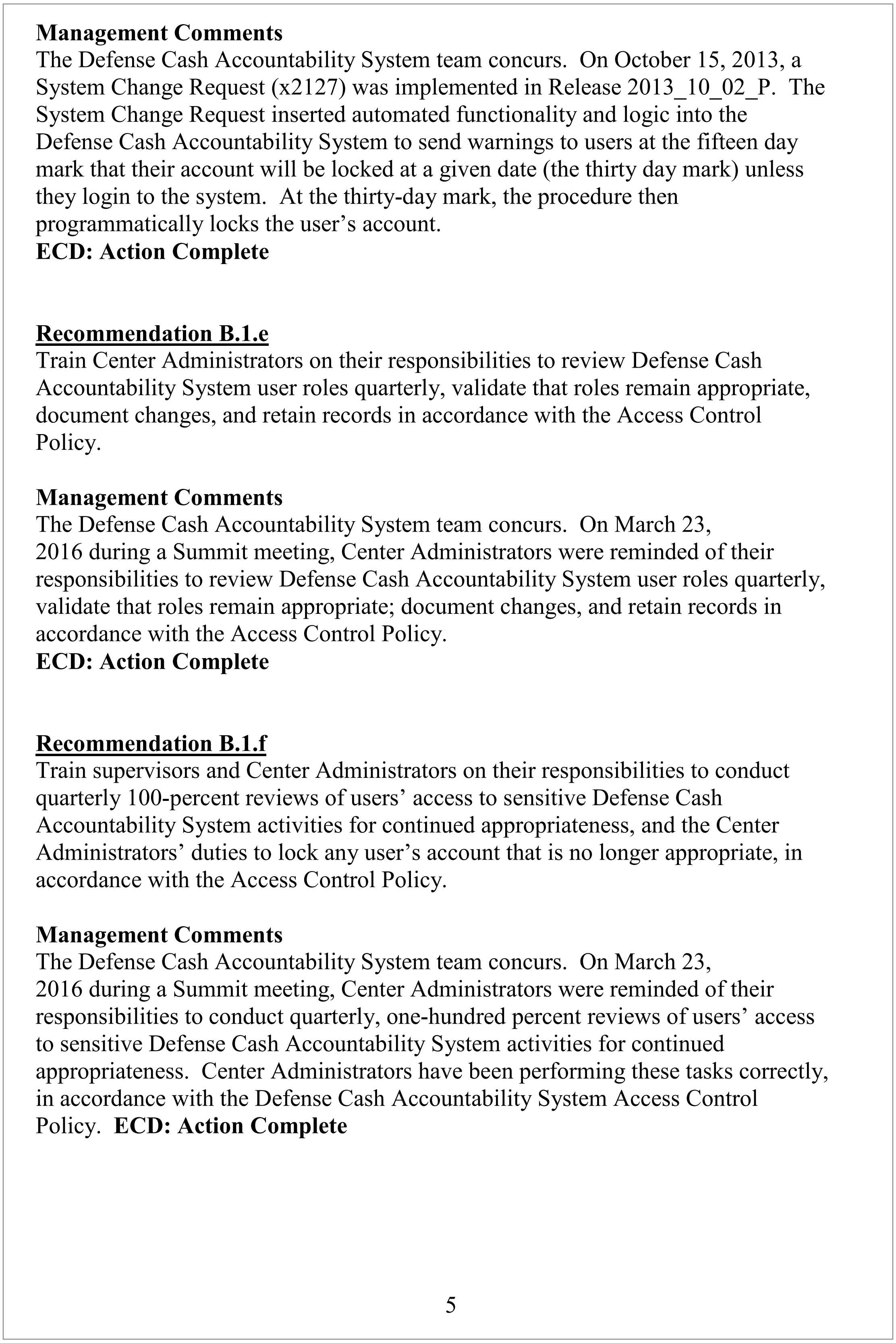
Recommendation B.1.c
Train Defense Cash Accountability System Information Assurance Officer Support Office personnel to return incomplete System Authorization Access Requests to the Center Administrators for additional review and completion before creating user accounts and granting access, in accordance with the Access Control Policy.

Management Comments
The Defense Cash Accountability System team concurs. In accordance with Federal Information System Controls Audit Manual (FISCAM), the applicable Information System Security Office personal have been trained and are currently completing reviews properly for System Authorization Access Requests, as stated in Defense Cash Accountability System Access Control Policy.

Effective October 21, 2016, all 'New User' and 'Modification' access requests will be processed in an automated Account Management and Provisioning System (AMPS). The Account Management and Provisioning System handles the role request approval process by supporting DD 2875 approval business processes that are followed by the Defense Finance and Accounting Service user communities. In the Account Management and Provisioning System, if a request is found to be incomplete, it can be rejected. A revalidation request will automatically be sent back to the user for more information. The user is then allotted thirty days from the date of the initial email notification to respond to a revalidation request.
ECD: Action Complete

Recommendation B.1.d
Train Center Administrators and Defense Cash Accountability System Help Desk personnel on their responsibilities and duties to terminate accounts of users who left the organization or had not accessed their accounts within 45 days.

Information and Technology, Defense Finance and Accounting Service (cont'd)



Management Comments
The Defense Cash Accountability System team concurs. On October 15, 2013, a System Change Request (x2127) was implemented in Release 2013_10_02_P. The System Change Request inserted automated functionality and logic into the Defense Cash Accountability System to send warnings to users at the fifteen day mark that their account will be locked at a given date (the thirty day mark) unless they login to the system. At the thirty-day mark, the procedure then programmatically locks the user's account.
ECD: Action Complete

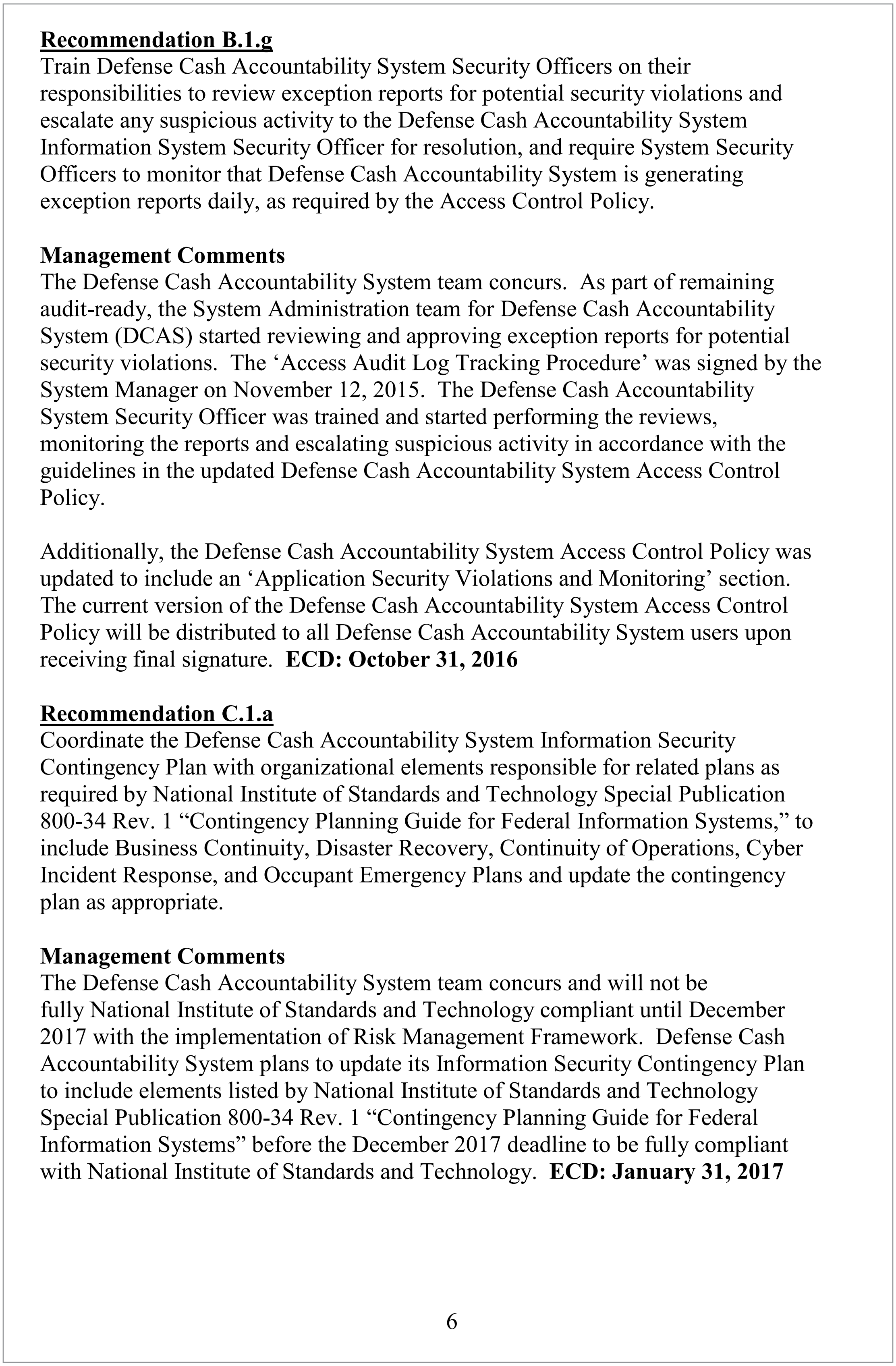
Recommendation B.1.e
Train Center Administrators on their responsibilities to review Defense Cash Accountability System user roles quarterly, validate that roles remain appropriate, document changes, and retain records in accordance with the Access Control Policy.

Management Comments
The Defense Cash Accountability System team concurs. On March 23, 2016 during a Summit meeting, Center Administrators were reminded of their responsibilities to review Defense Cash Accountability System user roles quarterly, validate that roles remain appropriate; document changes, and retain records in accordance with the Access Control Policy.
ECD: Action Complete

Recommendation B.1.f
Train supervisors and Center Administrators on their responsibilities to conduct quarterly 100-percent reviews of users' access to sensitive Defense Cash Accountability System activities for continued appropriateness, and the Center Administrators' duties to lock any user's account that is no longer appropriate, in accordance with the Access Control Policy.

Management Comments
The Defense Cash Accountability System team concurs. On March 23, 2016 during a Summit meeting, Center Administrators were reminded of their responsibilities to conduct quarterly, one-hundred percent reviews of users' access to sensitive Defense Cash Accountability System activities for continued appropriateness. Center Administrators have been performing these tasks correctly, in accordance with the Defense Cash Accountability System Access Control Policy. **ECD: Action Complete**

Information and Technology, Defense Finance and Accounting Service (cont'd)



Recommendation B.1.g
Train Defense Cash Accountability System Security Officers on their responsibilities to review exception reports for potential security violations and escalate any suspicious activity to the Defense Cash Accountability System Information System Security Officer for resolution, and require System Security Officers to monitor that Defense Cash Accountability System is generating exception reports daily, as required by the Access Control Policy.

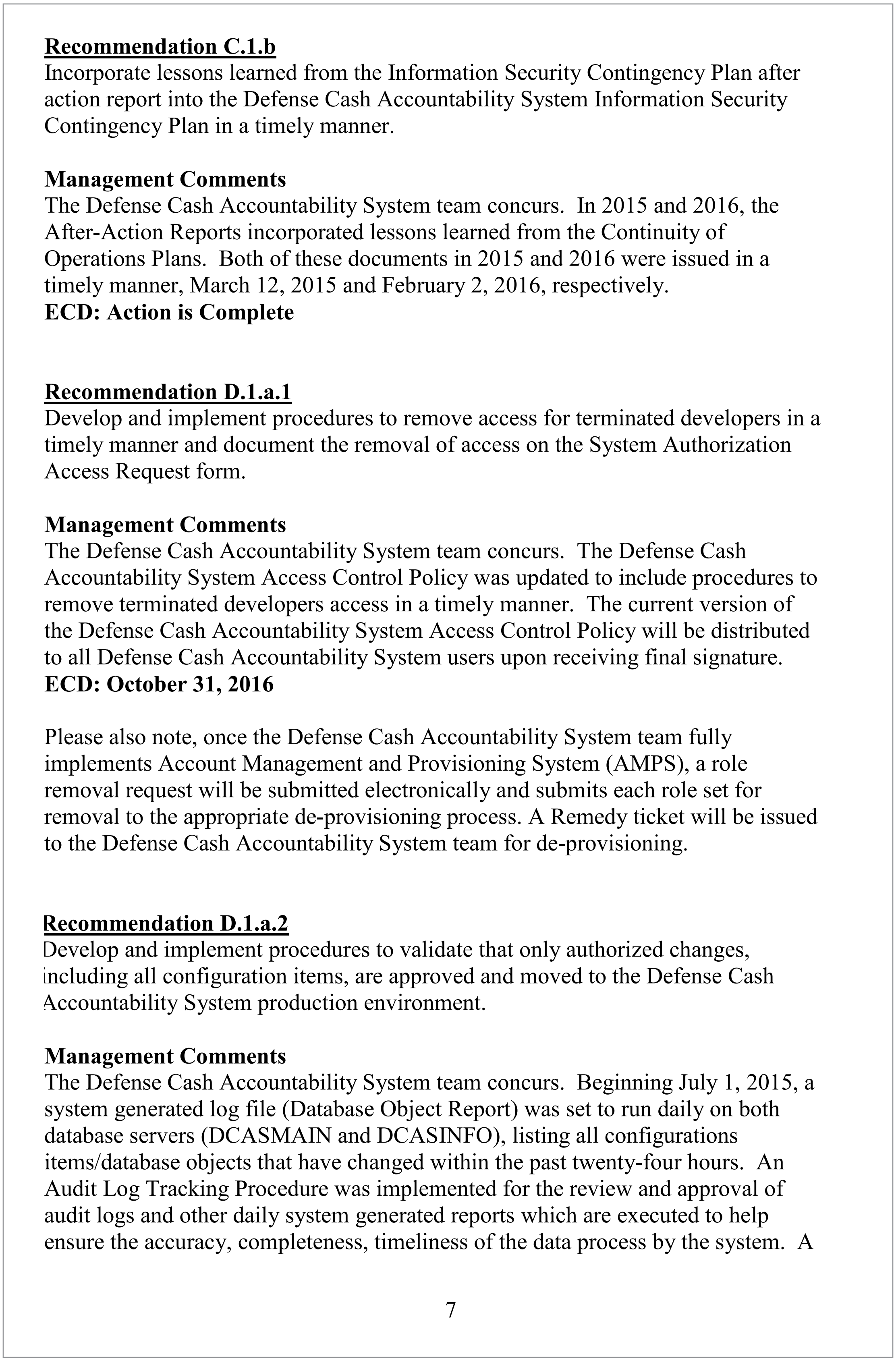
Management Comments
The Defense Cash Accountability System team concurs. As part of remaining audit-ready, the System Administration team for Defense Cash Accountability System (DCAS) started reviewing and approving exception reports for potential security violations. The 'Access Audit Log Tracking Procedure' was signed by the System Manager on November 12, 2015. The Defense Cash Accountability System Security Officer was trained and started performing the reviews, monitoring the reports and escalating suspicious activity in accordance with the guidelines in the updated Defense Cash Accountability System Access Control Policy.

Additionally, the Defense Cash Accountability System Access Control Policy was updated to include an 'Application Security Violations and Monitoring' section. The current version of the Defense Cash Accountability System Access Control Policy will be distributed to all Defense Cash Accountability System users upon receiving final signature. **ECD: October 31, 2016**

Recommendation C.1.a
Coordinate the Defense Cash Accountability System Information Security Contingency Plan with organizational elements responsible for related plans as required by National Institute of Standards and Technology Special Publication 800-34 Rev. 1 "Contingency Planning Guide for Federal Information Systems," to include Business Continuity, Disaster Recovery, Continuity of Operations, Cyber Incident Response, and Occupant Emergency Plans and update the contingency plan as appropriate.

Management Comments
The Defense Cash Accountability System team concurs and will not be fully National Institute of Standards and Technology compliant until December 2017 with the implementation of Risk Management Framework. Defense Cash Accountability System plans to update its Information Security Contingency Plan to include elements listed by National Institute of Standards and Technology Special Publication 800-34 Rev. 1 "Contingency Planning Guide for Federal Information Systems" before the December 2017 deadline to be fully compliant with National Institute of Standards and Technology. **ECD: January 31, 2017**

Information and Technology, Defense Finance and Accounting Service (cont’d)



Recommendation C.1.b
Incorporate lessons learned from the Information Security Contingency Plan after action report into the Defense Cash Accountability System Information Security Contingency Plan in a timely manner.

Management Comments
The Defense Cash Accountability System team concurs. In 2015 and 2016, the After-Action Reports incorporated lessons learned from the Continuity of Operations Plans. Both of these documents in 2015 and 2016 were issued in a timely manner, March 12, 2015 and February 2, 2016, respectively.
ECD: Action is Complete

Recommendation D.1.a.1
Develop and implement procedures to remove access for terminated developers in a timely manner and document the removal of access on the System Authorization Access Request form.

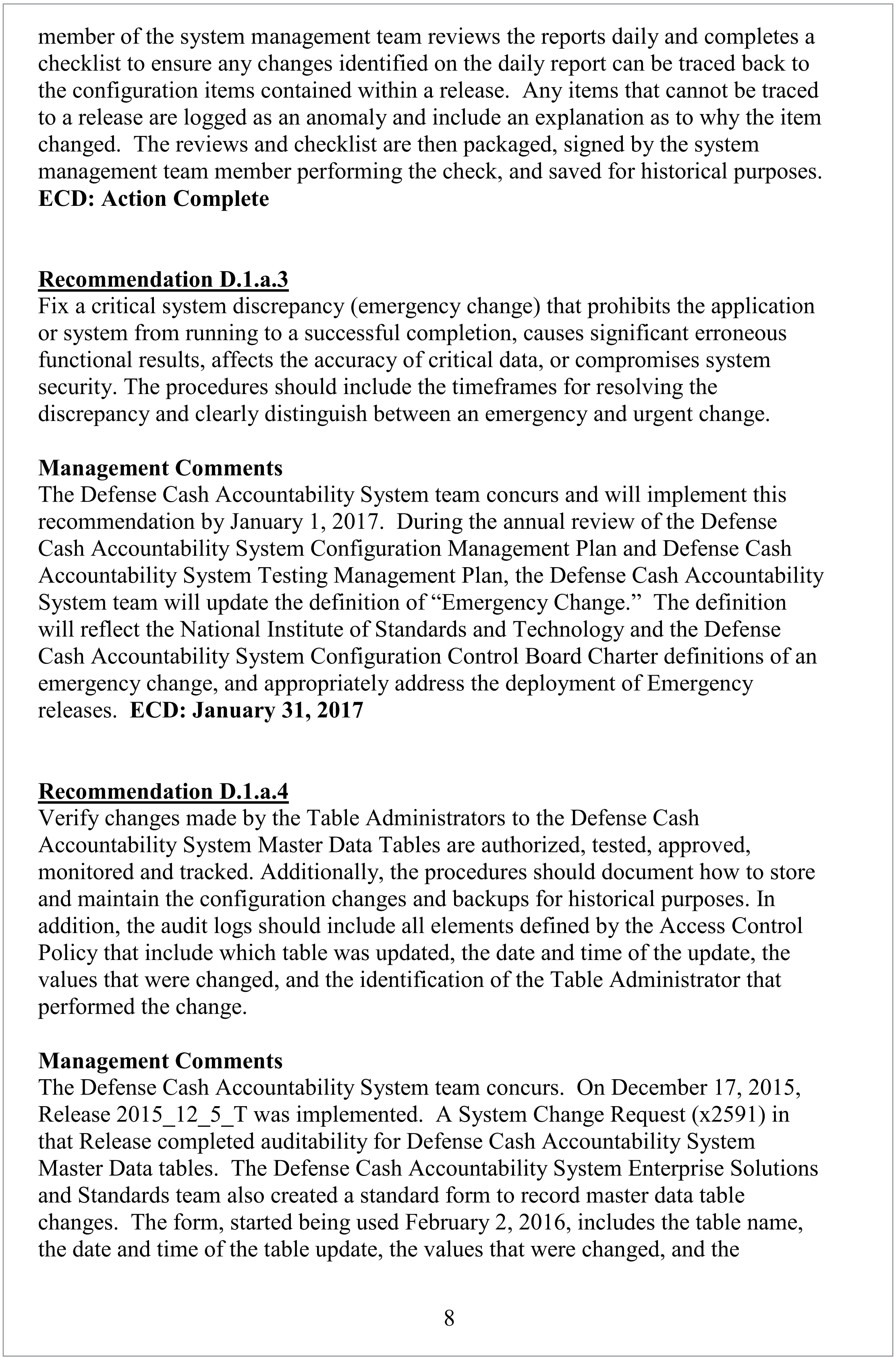
Management Comments
The Defense Cash Accountability System team concurs. The Defense Cash Accountability System Access Control Policy was updated to include procedures to remove terminated developers access in a timely manner. The current version of the Defense Cash Accountability System Access Control Policy will be distributed to all Defense Cash Accountability System users upon receiving final signature.
ECD: October 31, 2016

Please also note, once the Defense Cash Accountability System team fully implements Account Management and Provisioning System (AMPS), a role removal request will be submitted electronically and submits each role set for removal to the appropriate de-provisioning process. A Remedy ticket will be issued to the Defense Cash Accountability System team for de-provisioning.

Recommendation D.1.a.2
Develop and implement procedures to validate that only authorized changes, including all configuration items, are approved and moved to the Defense Cash Accountability System production environment.

Management Comments
The Defense Cash Accountability System team concurs. Beginning July 1, 2015, a system generated log file (Database Object Report) was set to run daily on both database servers (DCASMAIN and DCASINFO), listing all configurations items/database objects that have changed within the past twenty-four hours. An Audit Log Tracking Procedure was implemented for the review and approval of audit logs and other daily system generated reports which are executed to help ensure the accuracy, completeness, timeliness of the data process by the system. A

Information and Technology, Defense Finance and Accounting Service (cont'd)



member of the system management team reviews the reports daily and completes a checklist to ensure any changes identified on the daily report can be traced back to the configuration items contained within a release. Any items that cannot be traced to a release are logged as an anomaly and include an explanation as to why the item changed. The reviews and checklist are then packaged, signed by the system management team member performing the check, and saved for historical purposes. **ECD: Action Complete**

Recommendation D.1.a.3

Fix a critical system discrepancy (emergency change) that prohibits the application or system from running to a successful completion, causes significant erroneous functional results, affects the accuracy of critical data, or compromises system security. The procedures should include the timeframes for resolving the discrepancy and clearly distinguish between an emergency and urgent change.

Management Comments

The Defense Cash Accountability System team concurs and will implement this recommendation by January 1, 2017. During the annual review of the Defense Cash Accountability System Configuration Management Plan and Defense Cash Accountability System Testing Management Plan, the Defense Cash Accountability System team will update the definition of "Emergency Change." The definition will reflect the National Institute of Standards and Technology and the Defense Cash Accountability System Configuration Control Board Charter definitions of an emergency change, and appropriately address the deployment of Emergency releases. **ECD: January 31, 2017**

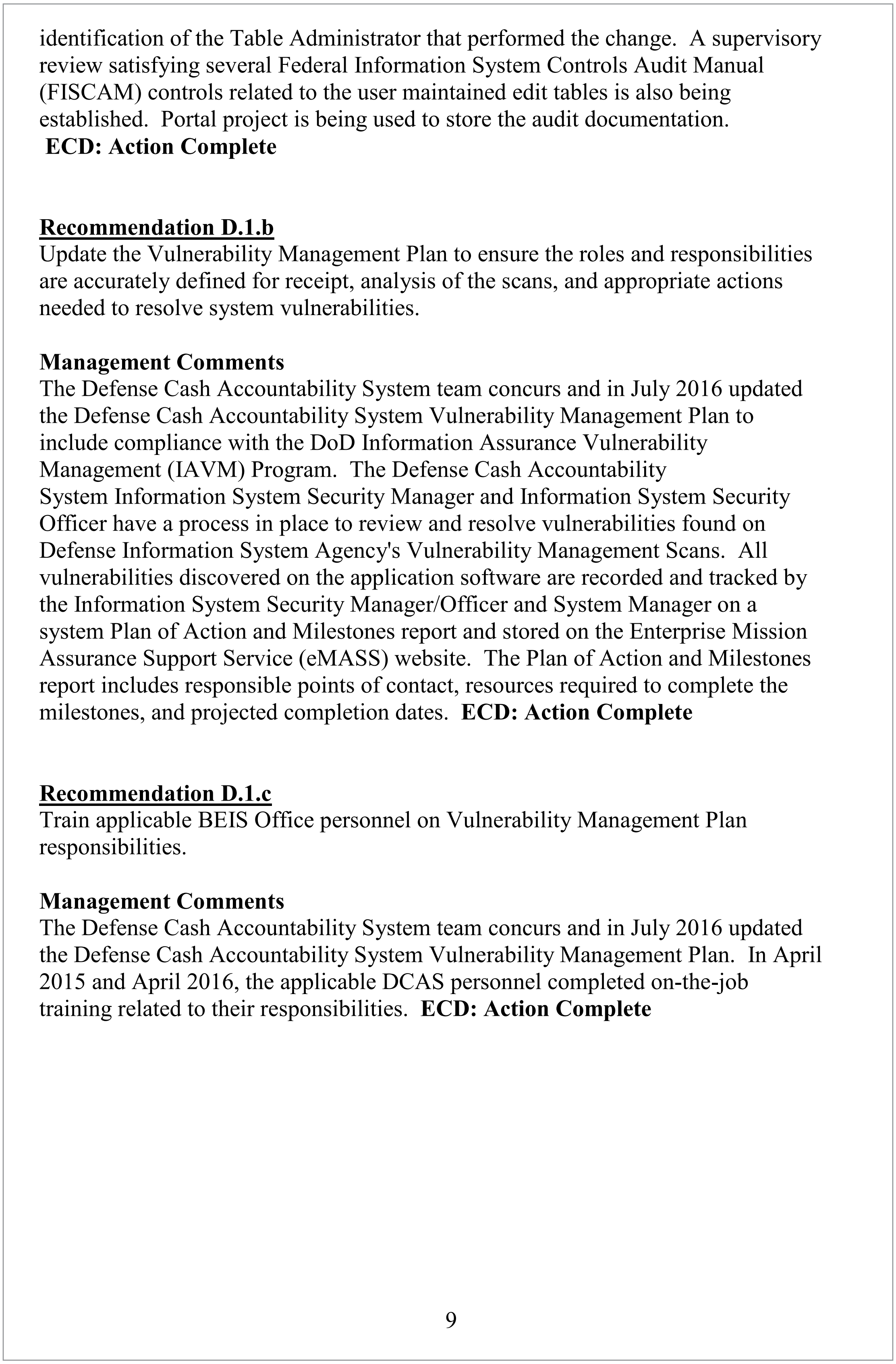
Recommendation D.1.a.4

Verify changes made by the Table Administrators to the Defense Cash Accountability System Master Data Tables are authorized, tested, approved, monitored and tracked. Additionally, the procedures should document how to store and maintain the configuration changes and backups for historical purposes. In addition, the audit logs should include all elements defined by the Access Control Policy that include which table was updated, the date and time of the update, the values that were changed, and the identification of the Table Administrator that performed the change.

Management Comments

The Defense Cash Accountability System team concurs. On December 17, 2015, Release 2015_12_5_T was implemented. A System Change Request (x2591) in that Release completed auditability for Defense Cash Accountability System Master Data tables. The Defense Cash Accountability System Enterprise Solutions and Standards team also created a standard form to record master data table changes. The form, started being used February 2, 2016, includes the table name, the date and time of the table update, the values that were changed, and the

Information and Technology, Defense Finance and Accounting Service (cont'd)



identification of the Table Administrator that performed the change. A supervisory review satisfying several Federal Information System Controls Audit Manual (FISCAM) controls related to the user maintained edit tables is also being established. Portal project is being used to store the audit documentation. **ECD: Action Complete**

Recommendation D.1.b

Update the Vulnerability Management Plan to ensure the roles and responsibilities are accurately defined for receipt, analysis of the scans, and appropriate actions needed to resolve system vulnerabilities.

Management Comments

The Defense Cash Accountability System team concurs and in July 2016 updated the Defense Cash Accountability System Vulnerability Management Plan to include compliance with the DoD Information Assurance Vulnerability Management (IAVM) Program. The Defense Cash Accountability System Information System Security Manager and Information System Security Officer have a process in place to review and resolve vulnerabilities found on Defense Information System Agency's Vulnerability Management Scans. All vulnerabilities discovered on the application software are recorded and tracked by the Information System Security Manager/Officer and System Manager on a system Plan of Action and Milestones report and stored on the Enterprise Mission Assurance Support Service (eMASS) website. The Plan of Action and Milestones report includes responsible points of contact, resources required to complete the milestones, and projected completion dates. **ECD: Action Complete**

Recommendation D.1.c

Train applicable BEIS Office personnel on Vulnerability Management Plan responsibilities.

Management Comments

The Defense Cash Accountability System team concurs and in July 2016 updated the Defense Cash Accountability System Vulnerability Management Plan. In April 2015 and April 2016, the applicable DCAS personnel completed on-the-job training related to their responsibilities. **ECD: Action Complete**

Acronyms and Abbreviations

ACP	Access Control Policy
AMPS	Account Management and Provisioning System
BEIS	Business Enterprise Information Services
CA	Center Administrator
DCAS	Defense Cash Accountability System
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
FISCAM	Federal Information Systems Control Audit Manual
FISMA	Federal Information Security Modernization Act
GAO	Government Accountability Office
I&T	Information and Technology
IA	Information Assurance
IAO	Information Assurance Officer
IO	Information Owner
ISSO	Information System Security Officer
NIST	National Institute of Standards and Technology
SAAR	System Authorization Access Request
SLA	Service Level Agreement
STIG	Security Technical Implementation Guide
U.S.C.	United States Code

Whistleblower Protection

U.S. Department of Defense

The Whistleblower Protection Ombudsman's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. The DoD Hotline Director is the designated ombudsman. For more information, please visit the Whistleblower webpage at 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
www.dodig.mil/pubs/email_update.cfm

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

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