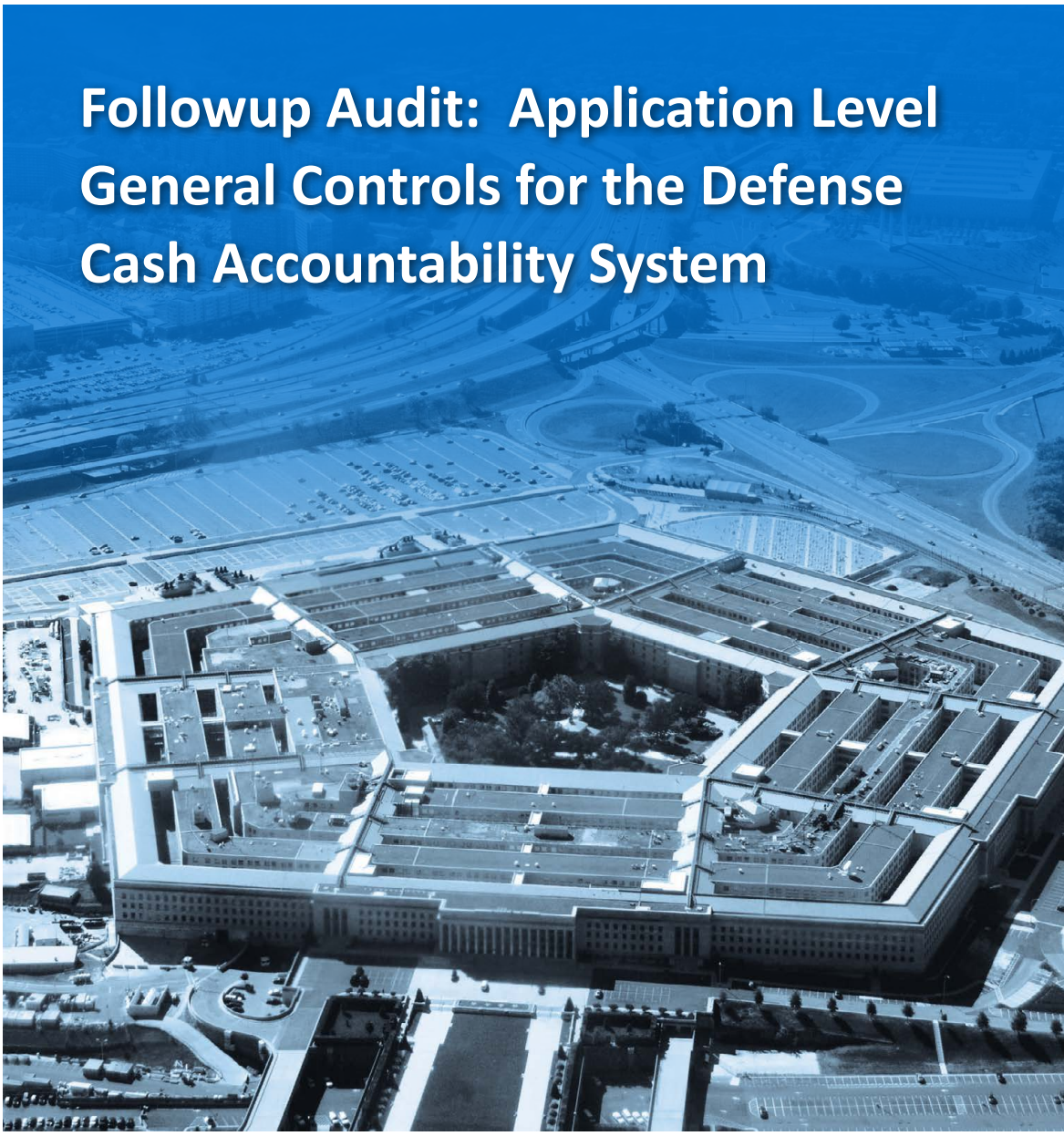
Report No. DODIG-2018-136

INSPECTOR GENERAL

U.S. Department of Defense

JULY 10, 2018

Followup Audit: Application Level General Controls for the Defense Cash Accountability System



INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

Followup Audit: Application Level General Controls for the Defense Cash Accountability System

July 10, 2018

Objective

We determined whether the Defense Finance and Accounting Service (DFAS) implemented corrective actions for the recommendations in Report No. DODIG-2017-015, "Application Level General Controls for the Defense Cash Accountability System Need Improvement," November 10, 2016, and determined whether those actions corrected the reported problems.[1]

Background

Report No. DODIG-2017-015 identified that the Defense Cash Accountability System (DCAS) application level general controls that DFAS administered in FY 2016 did not operate effectively. Specifically, we made 20 recommendations to mitigate vulnerabilities in security management, access, configuration management, and contingency planning controls.

Findings

Business Enterprise Information Services (BEIS) Office personnel implemented corrective actions that improved the design and operating effectiveness of several key application level general controls including security management, access controls, configuration management, and contingency planning. This occurred because BEIS Office personnel developed, revised, disseminated, and implemented policies and procedures and trained personnel on the specific requirements for application level general

[1] Application level general controls, also referred to as application security, consist of general controls operating at the business process application level and include security management controls, access controls, configuration management controls, contingency plans, and segregation of duties.

Findings (cont'd)

controls. As a result, selected controls were operating effectively to minimize risks associated with the intent of the controls, and 11 of 20 prior recommendations are closed.

Additionally, BEIS Office personnel made control design improvements in access and configuration management controls, meeting the intent of four additional recommendations, which are closed. However, BEIS Office personnel have not yet verified that four controls related to access and configuration management controls are operating as intended. BEIS Office personnel need to take additional actions to demonstrate the successful implementation of these controls. Without confirmation that these access and configuration management controls were operating as intended, DCAS remains vulnerable to inappropriate user access and critical system discrepancies.

Although these control enhancements closed 15 recommendations, BEIS Office personnel need to make additional improvements to security management, configuration management, and contingency planning controls. Also, we redirected one prior recommendation related to table change documentation from BEIS Office personnel to DFAS Enterprise Shared Services (ESS) personnel because DCAS policy requires DFAS ESS personnel to verify and track that Master Data Table changes are authorized, configured, and operating effectively.[2] Therefore, 5 of 20 prior recommendations remain open. Without proper controls, DCAS is vulnerable to availability interruptions and lost or incorrectly processed data. Consequently, the DoD could experience financial losses from expensive efforts to recover financial data, and DoD leadership's reliance on inaccurate or incomplete financial data processed to make critical decisions.

Finally, the Defense Information Systems Agency (DISA) Customer Service Representative did not perform the 2017 annual review of the DCAS Service Level Agreement to ensure agreements by all DCAS parties are still applicable

[2] Master data tables are sensitive data used to perform edits, verifications, and validations of data.

Results in Brief

Followup Audit: Application Level General Controls for the Defense Cash Accountability System

Findings (cont'd)

for the next 12 months.[3] This occurred because the Revenue Branch Chief did not instruct the DISA Customer Account Representative of the annual review requirement. As a result, necessary financial or service level changes may not occur, which could impact the performance of DCAS which DoD uses to process and report its disbursement and collection of funds to the U.S. Treasury and DoD.

Recommendations

As a result of our followup, we recommend that the DFAS BEIS and Other Systems Director:

- review and verify policies and procedures to execute periodic user reviews are operating effectively by documenting that 100 percent of sensitive users are reviewed each quarter and 100 percent of authorized users are reviewed within the last year;
- review and verify that privileged user reviews are conducted within consistent timeframes from the end of each quarter;
- refine, implement, and verify that the procedures for reviewing exception reports identify all exceptions that require followup or corrective actions;
- review and verify policies and procedures to execute and approve emergency changes as required;
- monitor the status of four open recommendations and expedite corrective actions to close them;[4]
- demonstrate that supervisors, Information Owners and their representatives, and Center Administrators have been trained to ensure that requested access levels to perform non-sensitive activities are appropriate before approving the System Authorization Access Requests and authorizing each user account; and
- coordinate with DISA to schedule and conduct the annual DCAS Information System Contingency Plan testing within a year of the prior testing.

In addition, we redirected one recommendation to the DFAS Operations Deputy Director to verify changes made by the Table Administrators to the DCAS Master Data Tables are authorized, tested, approved, monitored, and tracked.

We also recommend that the DISA Defense Working Capital Fund Revenue Branch Chief train DISA Enterprise Services personnel on the requirements of Service Level Agreement guidance, including annual review and documentation requirements.

Additionally, we recommend that the DISA Operations Center Financial Resource Management Office Chief develop and implement procedures to ensure annual Service Level Agreement reviews are conducted.

Management Comments and Our Response

The DFAS Information and Technology Director, responding for the DFAS BEIS and Other Systems Director, agreed with the recommendations to review, refine, implement, and verify policies and procedures to execute periodic user reviews, exception report reviews, and emergency changes consistently. Additonally, the

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

[4] Report No. DODIG-2017-015, "Application Level General Controls for the Defense Cash Accountability System Need Improvement," November 10, 2016, Recommendations B.1.b, A.1.c.1, D.1.a.4, and D.1.a.2.

Results in Brief

Followup Audit: Application Level General Controls for the Defense Cash Accountability System

Comments (cont'd)

Information and Technology Director agreed with the recommendation to coordinate with DISA to conduct annual DCAS Information System Contingency Plan testing no greater than every 12 months. Therefore, these recommendations are resolved but remain open. We will close the recommendations once we verify that BEIS Office personnel perform and document all user reviews consistently; that the reformatted exception report and revised procedures consistently identify exceptions; that the DCAS System Master Software Development Plan was updated to include emergency changes and the Configuration Control Board criteria; and that the DCAS Information System Contingency Plan was tested annually.

The DFAS Information and Technology Director, responding for DFAS BEIS and Other Systems Director, partially agreed with the recommendation to monitor the status of four open recommendations and expedite actions to close them. Specifically, the Information and Technology Director disagreed with the recommendation to require Information System Security Officers to comply with the certification requirements established in DoD Manual 8570.01-M.[5] The Information and Technology Director stated that DFAS separated account management functions from privileged system administration functions, and personnel in this role were erroneously included in the DoD Chief Information Office Cybersecurity Strategy Workforce, of which personnel require cybersecurity certification. We disagree that the account managers are not privileged users. Therefore, this recommendation is unresolved and remains open.

The DFAS ESS Director, responding for the DFAS BEIS and Other Systems Director, agreed with the recommendation to train Information Owners, their representatives, and Center Administrators to authorize appropriate access levels before approving each user account. Additionally, the DFAS ESS Director agreed with recommendations to verify changes made by the Table Administrators to the DCAS Master Data Tables are authorized, tested, approved, monitored, and tracked. Therefore, these recommendations are resolved but remain open. We will close the recommendations once we obtain documentation and verify that only appropriate access levels are authorized and DCAS Table Administrators make only authorized, tested, approved, monitored, and tracked changes to the DCAS Master Data Table.

The DISA Operations Center Financial Management Division Chief, responding for the DISA Defense Working Capital Fund Revenue Branch Chief, agreed with the recommendation to train the Operations Center Financial Management Division personnel for Service Level Agreement review and documentation requirements. Additionally, the Chief agreed with the recommendation to develop and implement procedures to ensure the DISA Customer Account Representative conducts and documents the annual SLA review as required, stating that the Customer Account Representative Desk Guide was revised accordingly. Therefore, these recommendations are resolved but remain open. We will close the recommendations once we verify that the Desk Guide was revised and personnel review and update annual SLAs.

We request that the DFAS BEIS and Other Systems Director provide additional comments in response to this report. Please see the Recommendations Table on the next page.

[5] DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Program," Incorporating Change 4, November 10, 2015.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Director, Business Enterprise Information Services and Other Systems, Defense Finance and Accounting Service	B.1.a	A.1.a, A.1.b, A.1.c, A.1.d, B.1.b, B.1.c	None
Deputy Director, Operations, Defense Finance and Accounting Service		B.2	None
Revenue Branch Chief, Defense Working Capital Fund, Defense Information Systems Agency		A.2	None
Chief, Operations Center Financial Management Division, Defense Information Systems Agency		A.3	None

Please provide Management Comments by August 9, 2018.

Note: The following categories are used to describe agency management's comments to individual recommendations.

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

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

July 10, 2018

MEMORANDUM FOR CHIEF INFORMATION OFFICER, DEFENSE FINANCE AND ACCOUNTING SERVICE
DEPUTY DIRECTOR, OPERATIONS, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, BUSINESS ENTERPRISE INFORMATION SERVICES AND OTHER SYSTEMS, DEFENSE FINANCE AND ACCOUNTING SERVICE
CHIEF, MISSION PARTNER ENGAGEMENT OFFICE, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Followup Audit: Application Level General Controls for the Defense Cash Accountability System (Report No. DODIG-2018-136)

We are providing this report for your review and comment. We conducted this audit in accordance with generally accepted government auditing standards.

We considered management comments from the Defense Finance and Accounting Service's Director of Information and Technology and Director of Enterprise Solutions and Standards, and from the Defense Information Systems Agency's Operations Center Financial Management Division Chief on a draft of this report when preparing the final report. Their comments have been appended to this report.

DoD Instruction 7650.03 requires that all recommendations be resolved promptly. Therefore, we request the that Defense Finance and Accounting Service's Director of Business Enterprise Information Services and Other Systems provide additional comments on Recommendation B.1.a by August 9, 2018.

Please send a PDF file containing your comments to audfmr@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 cooperation and assistance received during the audit. Please direct questions to me at (703) 601-5945 (DSN 329-5945).

Lorin T. Venable

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

Contents

Introduction

Objective

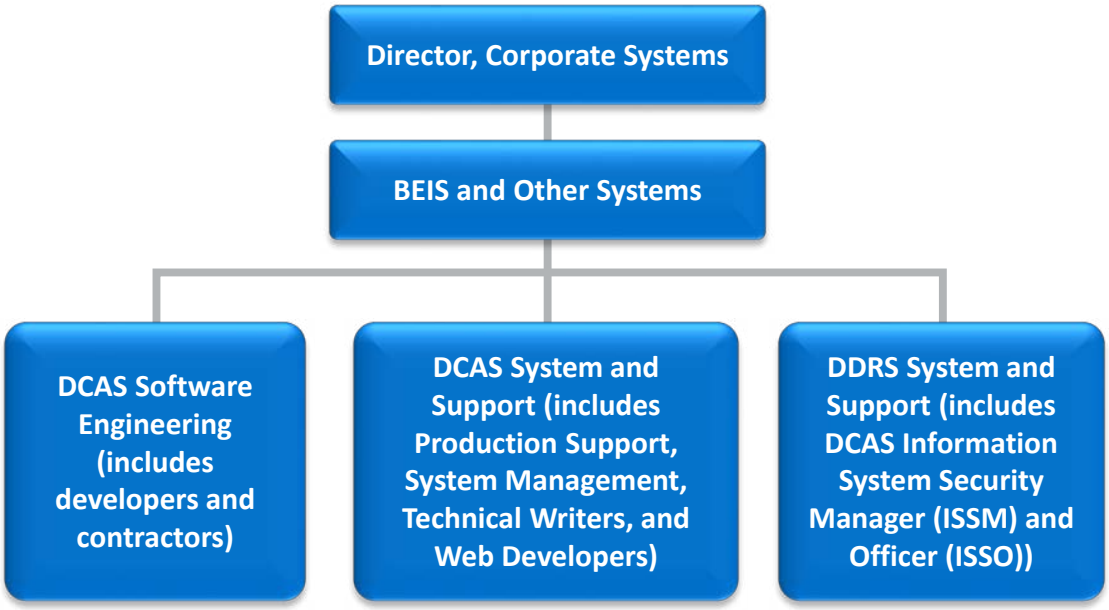
We determined whether the Defense Finance and Accounting Service (DFAS) implemented corrective actions for the recommendations in Report No. DODIG-2017-015, "Application Level General Controls for the Defense Cash Accountability System Need Improvement," November 10, 2016, and determined whether those actions corrected the reported problems. We performed this review in response to the Defense Cash Accountability System (DCAS) Program Office, which requested followup and verification that corrective actions were implemented and recommendations could be closed. See Appendix A for a discussion of the scope, methodology, and prior coverage related to the objective.

Background

The DoD uses DCAS to process and report its disbursement and collections of funds to the U.S. Treasury and the DoD. DCAS receives financial transaction data recorded from various DoD entity feeder systems, validates the accuracy of the data, and sends the data to appropriate DoD entity accounting systems. Monthly, DCAS processes more than 2 million transactions and 600 reports with over 14,000 files processed.

DCAS is managed by the DFAS Business Enterprise Information Services and Other Systems branch (BEIS Office personnel). This branch reports to the Corporate Systems Director, and is part of the DFAS Information and Technology directorate. The BEIS and Other Systems branch performs the technical duties, including those associated with DCAS configuration changes, review and correction of system-generated error messages, and system management. See the following figure for the reporting structure of the DFAS Corporate Systems Director.

Figure. DFAS Corporate Systems Organization Structure



Source: The DoD OIG.

The Enterprise Financial Information Services branch, which is part of the Enterprise Solutions and Standards division of DFAS, performs the operational duties of DCAS. Operational duties include providing oversight of periodic user reviews and making Master Data Table changes to the DCAS application without going through the configuration management process, when appropriate.

The Defense Information Systems Agency (DISA) provides DFAS hardware and software support for DCAS using a Service Level Agreement (SLA).[6] The DCAS System Manager, a member of the BEIS and Other Systems branch, coordinates changes to the SLA through the DISA Customer Account Representative, who is the primary point of contact with DISA for SLAs.

Information System Security Controls

Information system controls are generally divided into two categories—general controls and business process application controls. General controls are applied at the entity-wide, system, and business process application levels. These controls provide the policies and procedures that help ensure proper operations, such as physical security, which safeguard system hardware. Business process application controls provide the completeness, accuracy, validity, confidentiality, and availability of transactions and data during application processing.

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

Our review focused on the DCAS application level general controls, also referred to as application security, which is a control category under business process application controls. Application level general controls operate at the business process application level and 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 operations and assets of the agency to minimize potential damage and interruptions; and
- 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.

The effectiveness of general controls at the entity-wide and system levels is a significant factor in determining the effectiveness of business process controls at the application level. Weaknesses in entity-wide and system level general controls can result in unauthorized changes to business process applications and data that can bypass or weaken the success of application level controls.

Security Control Guidelines

Each Federal agency is required to comply with Federal Information Security Modernization Act and related policies, procedures, standards, and guidelines.[7] 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). NIST Special Publication 800-53 stipulates the guidelines that apply to all Federal information systems.[8] NIST Special Publication 800-53 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. The controls are customizable and implemented

[7] Public Law No. 113-283, "Federal Information Security Modernization Act of 2014," December 18, 2014.

[8] NIST Special Publication 800-53 Rev. 4, "Security And Privacy Controls for Federal Information Systems and Organizations," April 2013, including updates as of January 22, 2015; excludes national security systems as defined by 44 U.S.C § 3542.

as part of an organization-wide process that manages information security and privacy risk. These NIST controls are tested using the Government Accountability Office Federal Information System Controls Audit Manual (FISCAM). We used the Government Accountability Office FISCAM controls to evaluate the effectiveness of general and application controls. See Appendix A for additional information on the scope and methodology.

Summary of Prior Audit

We audited the application level general controls for DCAS in FY 2016 and found that the DCAS general controls administered by DFAS did not operate effectively.[9] Specifically:

- BEIS Office personnel did not properly approve and train Information System Security Officers (ISSOs) or review compliance with the SLA (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);
- 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, and document what those actions were and how they should have been implemented (Configuration Management).

DCAS application general controls administered by DFAS did not operate effectively because BEIS Office personnel did not follow the DCAS Access Control Policy (ACP), ensure comprehensive procedures to consistently operate and maintain DCAS existed, or train DFAS staff on the specific requirements to successfully implement trustworthy controls. As a result, DCAS had an increased risk that users accessed DCAS without authorization or the correct level of privileges. In addition, the control weaknesses identified could circumvent segregation of duties controls, which were operating as intended. Without proper controls, DCAS was vulnerable to availability interruptions and lost or incorrectly processed data. Losing the capacity to process, retrieve, and protect electronically maintained data can

[9] Report No. DODIG-2017-015, "Application Level General Controls for the Defense Cash Accountability System Need Improvement," November 10, 2016.

significantly affect the DoD's ability to accomplish its mission. Consequently, the DoD could experience financial losses from expensive efforts to recover financial data, and DoD leadership's reliance on inaccurate or incomplete financial data processed to make critical decisions.

Recommendations and Agreed-Upon Actions

In the prior report, we made 20 recommendations, all of which were resolved, but remained open.[10] The intent of these recommendations was to improve control design and operating effectiveness of DCAS application level general controls. The DFAS Information and Technology Director, responding for the DFAS BEIS and Other Systems Director, agreed with the recommendations, and agreed to take corrective actions by January 31, 2017. See Appendix B for a listing of recommendations from Report No. DODIG-2017-015.

Review of Internal Controls

DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and evaluates the effectiveness of the controls.[11] We identified continued internal control weaknesses associated with security management, access controls, configuration management, and contingency planning. We will provide a copy of the report to the senior officials responsible for internal controls.

[10] If a recommendation is resolved, it means management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation. Recommendations remained open until the OIG verified that the agreed-upon corrective actions were implemented.

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

Finding A

Corrective Actions Improved Several Key Application Level General Controls

BEIS Office personnel implemented corrective actions that improved the design and operating effectiveness of several key application level general controls including security management, access controls, configuration management, and contingency planning. This occurred because BEIS Office personnel developed, revised, disseminated, and implemented policies and procedures and trained personnel on the specific requirements for application level general controls. As a result, selected controls were operating effectively to minimize risks associated with the intent of the controls, and 11 of 20 prior recommendations are closed.

Additionally, BEIS Office personnel made control design improvements in access and configuration management controls, meeting the intent of four additional recommendations, which are closed. However, BEIS Office personnel have not yet verified that these controls are operating as intended. BEIS Office personnel need to take additional actions to demonstrate the successful implementation of these controls. Without confirmation that these access and configuration management controls were operating as intended, DCAS remains vulnerable to inappropriate user access and critical system discrepancies.

Controls Designed and Verified to be Operating Effectively

Federal internal control standards state that an effective internal control system provides reasonable assurance that the organization will achieve its objectives.[12] BEIS Office personnel designed and implemented corrective actions that improved the operating effectiveness of the nine key application level general controls discussed below. The implementation of the following nine security management, access, configuration management, and contingency planning controls resulted in the closure of 11 recommendations. See Appendix B for the status of recommendations from Report No. DODIG-2017-015.

[12] GAO-14-704G, "Standards for Internal Control in the Federal Government," September 2014.

Information Assurance Training Policy

BEIS Office personnel improved the DCAS security management control over Information Assurance (IA) awareness training and ensured an effective process to communicate DCAS policies was in place. This occurred because BEIS Office personnel developed and issued the DFAS IA training policy.[13] The DFAS Instruction assigns staff member responsibilities to ensure DFAS employees obtain the standard DFAS Cyber Awareness training and periodic refresher training.

BEIS Office personnel used reports provided by Human Resources to track DCAS users who did not complete annual IA training. The DFAS Human Resources Learning Development division sent DFAS personnel and their supervisors or Government points of contact automated e-mail reminders that mandatory training deadlines were approaching or passed. Additionally, BEIS Office personnel e-mailed both employees and supervisors when the IA training was past due. As a result, we concluded that these actions met the intent of Report No. DODIG-2017-015 Recommendation A.1.a to develop and disseminate a formal IA training policy for DCAS users. Because BEIS Office personnel completed the recommended action and we verified the updated policy and emails used to issue and implement the policy, this recommendation is closed.

Information System Security Officer Identification

BEIS Office personnel improved the DCAS security management control over identification of Administrative ISSOs and ensured the DCAS policies addressed responsibilities necessary to manage security. This occurred because BEIS Office personnel revised the DCAS ACP to appropriately identify that, based on their job duties, Center Administrators should be considered Administrative ISSOs.

The DCAS ACP describes DCAS application-specific access controls and establishes the framework that supports DCAS access, authorization, and authentication. According to the DCAS ACP, privileged users monitor and maintain DCAS user access. The privileged users are DCAS Center Administrators, DCAS System Administrators, and DCAS System Security Officers. We compared a DCAS system-generated list of users assigned these roles within DCAS to appointment letters and did not identify any discrepancies. As a result, we concluded that this action met the intent of Report No. DODIG-2017-015 Recommendation A.1.b to review the DCAS ACP, determine if it is appropriate for all Center Administrators to be ISSOs and, depending on the appropriateness of the policy, either implement the procedures or update the policy to identify who should be Administrative ISSOs. Because BEIS Office personnel completed the recommended action and we verified the updated policy, this recommendation is closed.

[13] DFAS Instruction 8570.01-I, "Cybersecurity (CS) Training and Certification Workforce Improvement Program (WIP)," August 10, 2015.

Service Provider Compliance

The DCAS System Manager improved the DCAS security management control over monitoring third-party provider compliance and ensured a process was in place to maintain oversight. This occurred because the DCAS System Manager signed a revised DCAS ACP that appropriately identified monitoring third-party provider compliance as a duty of the DCAS System Manager.

According to the DCAS ACP, one of the DCAS System Manager's duties is to ensure that DISA complied with services that were documented in the SLA. The SLA is a formal contract between DFAS and DISA that defines roles and responsibilities and provides a description of the service environment, service levels and costs, compliance and remedies for noncompliance, and period of performance. The DCAS System Manager provided email records that demonstrated he requested the DISA Customer Account Representative update the SLA. Specifically, the DCAS System Manager requested the SLA be updated to clearly define DISA and DFAS responsibilities for installing operating system and database patches and upgrades. Although he did not document the evaluation process through periodic reports, compliance reports, end user evaluations, or metrics, the DCAS System Manager met the intent of the NIST Special Publication 800-35, "Guide to Information Technology Security Services," requirement to develop a process for measuring and monitoring SLA compliance by demonstrating that he repeatedly requested SLA updates from the DISA Customer Account Representative. This action met the intent of Report No. DODIG-2017-015 Recommendation A.1.c.2 to develop and implement procedures to review the DCAS service provider's compliance with the terms in the SLA and was in accordance with the NIST. Because the DCAS System Manager completed the recommended actions and we verified the policy revision and implementation, this recommendation is closed.

Justification for Logout Exceptions

BEIS Office personnel improved the DCAS access control over user account locks and ensured the DCAS policies documented and validated mission requirements. This occurred because BEIS Office personnel revised the DCAS ACP appropriately to justify why production support staff roles require unlimited idle time.

The DCAS ACP states that the DCAS Information and Technology Production Support staff members do not have a timeout length for database connections for inactivity because the team is responsible for:

- monitoring the global team e-mail box and responding to user issues;
- resolving issues that will hold up or prevent daily grouping of records into batches from completing, and system-generated error messages;

- making configuration changes within authorized release events;
- coordinating operating system account actions with DISA; and
- resolving account access issues and remedy tickets.

The DCAS ACP identified those users, including production support users, who were approved to have the unlimited idle time and provided the justification to support the access request. This action met the intent of Report No. DODIG-2017-015 Recommendation B.1.a to 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 access request. Because BEIS Office personnel appropriately revised the DCAS ACP to address the recommendation and we verified and agreed with the revised policy justification, this recommendation is closed.

Authorizing DCAS Users

BEIS Office personnel improved the DCAS access control over appropriate authorization of DCAS users and ensured users level of access had been properly authorized. This occurred because BEIS Office personnel revised the DCAS ACP to require all users to complete the System Authorization Access Request (SAAR) using the automated application, Accounts Management and Provisioning System (AMPS). By implementing the automated application and its functionality, DCAS ensures user requests are properly routed and approved by appropriate individuals prior to granting access. Therefore, these actions met the intent of our prior recommendation, which was to validate that the SAAR was reviewed and properly approved by appropriate individuals.

The SAAR, formerly the DD Form 2875, documents that user access prerequisites have been met prior to granting access and maintains a proper document audit trail. AMPS requires users to complete all fields marked with a red asterisk before the SAARs can proceed to authorization and DFAS can grant access to DCAS. According to the AMPS User Guide, AMPS automatically creates and numbers a SAAR and forwards the SAAR to a sequence of approvers who have been assigned the appropriate AMPS administrative roles, which authorize the approvers to approve or deny the request.[14] When data warrants approving the request, the approvers certify the request in sequence, from the supervisor to the Security Officer to the Data Owner, concluding with the IA Officer.

[14] "AMPS Procedures for Users and Administrators," Version 3.2, January 27, 2016.

DFAS ESS personnel confirmed that all DCAS users were processing access requests through AMPS, and that paper SAARs were no longer used. According to DFAS ESS personnel, they confirmed this by comparing a list of DCAS users to a list of AMPS users. During this review, DFAS ESS personnel identified DCAS users who did not have SAARs in AMPS. DFAS ESS personnel notified those users that their DCAS access would be terminated on August 31, 2017, unless they completed SAARs in AMPS. We reviewed this information and determined that DFAS ESS personnel demonstrated that they verified 100 percent of DCAS users had SAARs in AMPS. These actions met the intent of Report No. DODIG-2017-015 Recommendation B.1.c to train DCAS IA Officer Support Office personnel to return incomplete SAARs to the Center Administrators for additional review and completion before creating user accounts and granting access, in accordance with the ACP. Because BEIS Office personnel completed actions that addressed the underlying concerns related to authorizing DCAS access levels and we verified the implemented automation of the process, this recommendation is closed.

Separated User Access Timely Termination

BEIS Office personnel improved the DCAS access control over terminating access within 45 days after a user was separated from employment and ensured access was disabled or removed in a timely manner. This occurred because BEIS Office personnel implemented an automated system deactivation at the 30-day mark, which disables an unauthorized user access to the system. By implementing the automated deactivation, Center Administrators and DCAS Help Desk personnel no longer are required to manually terminate accounts of users. These actions eliminated the need for training and this meets the intent of our prior training recommendation.

According to the DCAS ACP, DCAS is programmed to send warnings to users at the 15-day mark that their accounts will be locked at a given date, indicating the 30-day mark, unless they login to the system. At the 30-day mark, DCAS is programmed to lock the inactive users' accounts, and deactivates accounts that are inactive in excess of 45 days.[15]

While the previous DCAS ACP required the DCAS Help Desk/Operations Support team (DCAS Help Desk) to conduct monthly reviews to ensure terminated and inactive users no longer had access to DCAS, the revised policy relies solely on the automated logic of DCAS. We reviewed the program logic and verified the automated process was implemented. By relying on the automated process of AMPS, the BEIS Office personnel deleted the ACP requirement to conduct monthly reviews of terminated and inactive users and removed the need to

[15] As required by U.S. Cyber Command Tasking Order 13-0641, which affects all systems and applications under the DoD.

provide such training. This action met the intent of Report No. DODIG-2017-015 Recommendation B.1.d to train Center Administrators and DCAS 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. BEIS Office personnel completed the recommended actions that met the intent of our training recommendation, and we verified that the action taken addressed the control deficiency; therefore, this recommendation is closed.

Contingency Plan Coordination

The DFAS policy improved the DCAS contingency plan control over coordinating its plan with organizational elements responsible for related plans and ensured the plans incorporated the contingency plan.[16] This occurred because BEIS Office personnel implemented the October 2014 DFAS policy that requires the Information and Technology Director to participate in the development and execution of agency continuity plans. Additionally, the continuity plan was part of the package submitted to receive an Authority to Operate.

DFAS guidance defines the Authority to Operate as the official senior management decision to authorize operation of an information system.[17] By authorizing a system to operate, the senior official explicitly accepts the risk to organizational operations, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. The agreed-upon set of security controls are defined in NIST Special Publication 800-37, revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010. The DFAS Information and Technology Director approves the DCAS Authority to Operate after thoroughly reviewing the entire package submitted.

According to the NIST, the Contingency Plan Coordinator should evaluate supporting plans to ensure that the information is current and continues to meet system requirements adequately.[18] Additionally, the NIST requires the organization to coordinate contingency plan development with organizational elements responsible for related plans to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

[16] DFAS Directive 3020.26-DV, "DFAS Continuity Program," October 31, 2014.

[17] DFAS Instruction 8510.01-I, "Risk Management Framework (RMF)," November 10, 2015.

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

There was no specific documentation provided during this review to prove that the DCAS Information System Contingency Plan (ISCP) had been incorporated into related plans, such as the Disaster Recovery, Business Continuity, and Business Resumption Plans. However, the DCAS ISCP is part of the authorization package submitted to the Information and Technology Director to obtain an Authority to Operate. Based on DFAS policy, the Information and Technology Director participates in the development and execution of agency continuity plans. Therefore, the Information and Technology Director has the DCAS ISCP knowledge that he can use when participating in the agency continuity plan process. According to the NIST, the ISCP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system. Therefore, the DFAS policy requirements and the DoD Information Assurance Certification and Accreditation Process documents and approvals demonstrate that DFAS has met the intent of this control.[19] As a result, DFAS met the intent of Report No. DODIG-2017-015 Recommendation C.1.a to coordinate the DCAS information security contingency plan with organizational elements responsible for related plans and update the plan as appropriate. Because BEIS Office personnel completed the recommended action and we verified the coordination, this recommendation is closed.

Developer Access Termination

BEIS Office personnel improved the DCAS user account control over terminating developer access and ensured users were assigned to roles designed to prevent inappropriate access. This occurred because BEIS Office personnel revised the DCAS ACP to include procedures for terminating developer access and these procedures were implemented.

The DCAS ACP describes the supervisor's responsibilities for removal of access when a user transfers or realigns to another organization within DFAS where system access is still required (at a minimum of 30 days) or immediately upon notification when a user no longer requires system access. Additionally, the DCAS ACP states that the supervisor should follow DISA's policy and submit a SAAR requesting deactivation for each separate Information and Technology user account.

[19] The DoD Information Assurance Certification and Accreditation Process was the DoD procedures for identifying, implementing, validating, certifying, and managing information assurance controls, and authorizing the operation of DoD information systems. However, these procedures were rescinded on March 12, 2014, with the issuance of the Risk Management Framework. DCAS is still operating under the DoD Information Assurance Certification and Accreditation Process because BEIS Office personnel are following a transition timeline issued by the DoD Chief Information Officer that does not require them to fully transition to the Risk Management Framework until 2018.

DFAS has developed and implemented procedures in the DCAS ACP and the DFAS Information and Technology System Access Policy to remove access for terminated developers in a timely manner and document the removal of access on the SAAR form. We verified that these revised policies describe how access for terminated developers will be removed, how the removal will be documented, and the timeframes for removal. To verify that the revised policies had been implemented, we compared an organizational chart to a system-generated list of developers, based on access privileges. From that comparison, we identified two developers who, according to the revised DCAS ACP, should have had their developer access terminated. Therefore, we reviewed the SAARs for when access was removed, and determined BEIS Office personnel implemented the policy. This action met the intent of Report No. DODIG-2017-015 Recommendation D.1.a.1 to develop and implement procedures to remove access for terminated developers in a timely manner and document the removal of access on the SAAR form. Because BEIS Office personnel completed the recommended action and we verified the implementation of the revised procedures, the recommendation is closed.

Vulnerability Management Plan

BEIS Office personnel improved the DCAS configuration management controls over the vulnerability management plan and ensured the process effectively identified vulnerabilities.[20] This occurred because BEIS Office personnel revised the Vulnerability Management Plan. This revision included defining roles and responsibilities for scan report receipt, analysis of the vulnerability scans, and appropriate actions needed to resolve system vulnerabilities. Although the DCAS ISSO did not receive formal training for the Vulnerability Management Plan, the DCAS ISSO received training from DISA on reading the scan results described in the plan.

NIST states that organizations should scan for vulnerabilities in the information system and hosted applications, and should perform scans when new vulnerabilities that could affect the system or applications are identified and reported.[21] NIST also states that organizations should analyze vulnerability scan reports and results from security control assessments. Finally, organizations should remediate legitimate vulnerabilities in accordance with an organizational risk assessment.

[20] NIST Special Publication 800-53 defines a vulnerability as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

[21] NIST Special Publication 800-53 Rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013.

We reviewed the revised plan, and verified it defined the roles and responsibilities for receipt, analysis of the scans, and appropriate actions needed to resolve system vulnerabilities. By comparing reports run at different times, we confirmed the DCAS ISSO was researching and resolving potential vulnerabilities. Therefore, these actions met the intent of Report No. DODIG-2017-015 Recommendations D.1.b and D.1.c to 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; and to train applicable BEIS Office personnel on Vulnerability Management Plan responsibilities. Because BEIS Office personnel completed the recommended actions and we verified the revised vulnerability management plan, these recommendations are closed.

Controls With Improved Design But Not Verified to be Operating Effectively

According to Federal internal control standards, a deficiency in internal control exists when the design, implementation, or operation of a control does not allow management or personnel, in the normal course of performing their assigned functions, to achieve control objectives and address related risks.[22] BEIS Office personnel made control design improvements in access and configuration management controls, meeting the intent of four additional recommendations. However, BEIS Office personnel have not yet verified that these controls are operating as intended. As a result, the four training recommendations for which BEIS Office personnel met the intent and satisfied the design of the controls are closed, but we made four new recommendations to verify that these new controls are operating effectively. See Appendix B for the status of recommendations from Report No. DODIG-2017-015.

Service Level Agreement Annual Reviews

The DFAS Information and Technology Director improved the DCAS security management control over SLA annual reviews and ensured provisions were developed to monitor compliance. This occurred because the DFAS Information and Technology Director required the DCAS System Manager to coordinate changes, if needed, and provide agreement with the DISA Customer Account Representative and maintained responsibility for the application's material within the SLA. Although BEIS Office personnel did not provide formal training, the DCAS System Manager provided documentation demonstrating his compliance with this expectation. This documentation included historic and current SLAs and email exchanges with the DISA Customer Account Representative in which the DCAS System Manager was consistently following up on the status of coordination.

[22] GAO-14-704G, "Standards for Internal Control in the Federal Government," September 2014.

The NIST requires managers to ensure that the service provider meets its stated service levels and complies with internal security policies and procedures.[23] Furthermore, according to the NIST, managers should conduct evaluations and document them through periodic reports, compliance reports, end user evaluations, or metrics. The DCAS System Manager discussed the annual SLA review on numerous occasions with the DISA Customer Account Representative. Based on the documented discussions, the DCAS System Manager complied with the annual review from a DFAS perspective. Even though BEIS Office personnel did not provide formal training, the actions taken by the DCAS System Manager met the intent of Report No. DODIG-2017-015 Recommendation A.1.d to ensure DFAS personnel review governance over support and mission work agreements and compliance with SLA requirements. Because BEIS Office personnel completed the recommended action and we verified the DCAS system manager's compliance, this recommendation is closed.

Although the DCAS System Manager complied with the annual review from a DFAS perspective, DISA did not perform the annual SLA review of DCAS as required by DISA guidance.[24] This occurred because the DISA Defense Working Capital Fund Revenue Branch Chief did not provide effective training to the DISA Customer Account Representative. In addition, the DISA Customer Account Representative did not coordinate a review of the DCAS application agreement with the DCAS System Manager within 12 months of the prior review.

According to DISA guidance:

- the DISA Customer Account Representative and the customer are required to review the agreement at least annually to determine whether any modifications or amendments are needed to reflect the customer's support requirements and DISA Customer Account Representative's furnished services;
- the DISA Customer Account Representative should always inquire and record what date the customer expects to have the SLA back to the DISA Customer Account Representative; and
- all annual reviews require the customer to annotate acknowledgement (the SLA annual review table), making the annual reviews bilateral agreements.

[23] NIST Special Publication 800-35, "Guide to Information Technology Security Services," October 2003.

[24] "Defense Working Capital Fund Service Level Agreement Guidance," March 2016.

The Revenue Branch Chief could not demonstrate compliance with the annual review requirement because the DISA Customer Account Representative had not initiated the 2017 annual review and, consequently, the DISA Customer Account Representative could not provide a record of the 2017 annual review.[25] The Revenue Branch Chief stated that inadequate training directly resulted in the DISA Customer Account Representative's failure to meet annual SLA reviews and annual review documentation requirements. She stated that training will be provided, but did not provide details or a timeline for the training. Without all parties completing the required annual SLA review, the DISA Customer Account Representative may not make necessary financial or service level changes, which could impact the performance of DCAS.

The Revenue Branch Chief should provide to the DISA Customer Account Representative training that includes annual SLA review and annual review documentation requirements. After the DISA Customer Account Representative completes the training, the DISA Operations Center Financial Resource Management Office Chief should develop and implement procedures to ensure the DISA Customer Account Representative conducts annual SLA reviews as required and document acknowledgement on the SLA annual review table.

Periodic Review of DCAS User Access

DFAS ESS personnel improved the DCAS access control over periodic reviews of user access, and BEIS Office personnel ensured the DCAS policies required personnel to periodically review user access privileges. This occurred because the BEIS Office personnel revised the DCAS ACP review requirements, and DFAS ESS personnel provided DCAS ACP training in May 2017. The training met the intent of Report No. DODIG 2017-015 Recommendations B.1.e and B.1.f to train:

- Center Administrators on their responsibilities to review DCAS user roles quarterly, validate that roles remain appropriate, document changes, and retain records in accordance with the ACP; and
- supervisors and Center Administrators on their responsibilities to conduct quarterly 100 percent reviews of users' access to sensitive DCAS activities for continued appropriateness, and the Center Administrators' duties to lock any user's account that is no longer appropriate, in accordance with the ACP.

[25] As of February 5, 2018.

Because BEIS Office and DFAS ESS personnel completed the recommended actions, these recommendations are closed. However, because the access review procedures were not in place until third quarter FY 2017, and the DCAS ACP requires 100 percent of authorized users to be reviewed annually, BEIS Office personnel will not be able to demonstrate the control is operating effectively until they verify that 100 percent of authorized users were reviewed within the last year, or third quarter FY 2018.

According to the DCAS ACP, BEIS Office personnel conduct quarterly user reviews. The requirements for quarterly user reviews were segmented into three different types of users for whom access was reviewed—authorized, sensitive, and privileged.

Access Reviews for Authorized Users

The DCAS ACP defines an authorized DCAS user as any appropriately cleared individual with a requirement to access DCAS in order to perform or assist in a lawful and authorized governmental function. Authorized users include DoD employees, contractors, and guest researchers.[26] According to the DCAS ACP, Administrative ISSOs obtain a system-generated listing of authorized users and conduct quarterly reviews to ensure end users still require access to DCAS. The review will be based on 100 percent of all end users (excluding sensitive users) on an annual basis. We did not test the authorized user reviews because the procedures were not in place until third quarter FY 2017, and the DCAS ACP requires 100 percent of authorized users to be reviewed annually. Therefore, the control did not have a full cycle of 1 year from which to effectively assess whether it was working correctly. As a result, even though DFAS ESS personnel provided training for conducting user access reviews, verification of the operating effectiveness of this control cannot be completed until third quarter FY 2018, when BEIS Office personnel document that 100 percent of authorized users were reviewed within the last year.

Access Reviews for Sensitive Users

The DCAS ACP defines a sensitive user as any user with an identified sensitive application role.[27] Activities are considered sensitive based upon the type of data being accessed: if the data being accessed is sensitive in nature, then the activity is also considered sensitive. According to the DCAS ACP, Administrative ISSOs obtain

[26] DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Program," Incorporating Change 4, November 10, 2015.

[27] Per the DCAS ACP, sensitive application roles include Source Data Administrator, Domain of Interest Scope Maintainer, Reference Table Administrator, Security Assistance Reference Table Administrator, TI-97 Reference Table Administrator, and users who have the ability to see personally identifiable information.

a system-generated listing of sensitive users and conduct quarterly reviews to ensure these users still require this level of DCAS access. The review will be based on 100 percent of all sensitive users on a quarterly basis. BEIS Office and DFAS ESS personnel provided data calls, lists of users, duplicate listings, and evidence of actions taken to address potentially unauthorized users for each center.[28] We met with DFAS ESS personnel to seek clarity for the documentation provided, yet DFAS ESS personnel could not explain how each center implemented the DCAS ACP requirements to conduct quarterly reviews. According to our review, each center used different procedures to conduct user reviews, which were inconsistent in the level of detail they could provide to support the review results and actions taken. For example, DFAS Rome was the only center of the four which maintained detailed records of all actions initiated because of the user reviews, including dates and accountable individuals. Additionally, without reasonable assurance that DFAS ESS personnel provided complete sensitive user populations to be reviewed each quarter, we determined sampling the authorized users was not useful. Additionally, DFAS ESS personnel did not provide consistent evidence of which sensitive users were reviewed and what actions were taken and why. Therefore, we did not perform any additional testing for the sensitive user reviews. As a result, even though DFAS ESS personnel provided training for conducting sensitive user access reviews, DFAS ESS personnel could not demonstrate that the controls over access reviews for sensitive users were operating effectively.

Access Reviews for Privileged Users

According to DoD Manual 8570.01-M, a privileged user is defined as an authorized user who has access to system control, monitoring, administration, criminal investigation, or compliance functions.[29] A new requirement was added to the DCAS ACP since our original audit, which requires the DCAS Information System Security Manager (ISSM), DCAS ISSO, or both, to perform quarterly user reviews for 100 percent of the DCAS privileged users. We requested evidence of the quarterly privileged user reviews. We ensured all privileged application users were identified to ensure 100 percent review, reviewed query logic for reports generated for review, last login dates (to ensure users were still active users), supervisor e-mails (to ensure job function alignment), and appointment letters (to ensure users had been delegated the authority to be privileged users). Based on this review, we determined that BEIS Office personnel did not complete the reviews in consistent timeframes. For example, BEIS Office personnel conducted three quarterly reviews during FY 2017, and completed the

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

[29] DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Program," Incorporating Change 4, November 10, 2015.

second quarter FY 2017 review on the quarter's closing date. However, BEIS Office personnel completed the third quarter FY 2017 review 21 days after the quarter's closing date. Additionally, BEIS Office personnel did not even initiate the fourth quarter FY 2017 review until 39 days after the quarter closing date. Although we did not identify any problems with the accuracy of the reviews, without consistent review timeframes privileged users may have maintained elevated DCAS access inappropriately without their need for this level of access. As a result, BEIS Office personnel could not demonstrate that the privileged user access review controls were operating effectively.

DFAS ESS personnel provided the training that met the intent of our recommendation, which mitigated the control design deficiency. However, DFAS ESS personnel could not demonstrate that the user access review controls were operating effectively. BEIS Office personnel should review and verify that their policies and procedures to execute periodic user reviews in accordance with the DCAS ACP are operating effectively by documenting that 100 percent of sensitive users were reviewed each quarter and 100 percent of authorized users were reviewed within the last year. Additionally, BEIS Office personnel should review and verify that privileged user reviews are conducted within consistent timeframes from the end of each quarter.

Application Security Violations Reports Monitoring

BEIS Office personnel improved the access controls design over security and violation monitoring (exception reports). This occurred because BEIS Office personnel trained the DCAS System Administrators on the intent and importance of monitoring user access. The on-the-job training BEIS Office personnel provided met the intent of Report No. DODIG-2017-015 Recommendation B.1.g to train DCAS 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 System Security Officers to monitor that DCAS is generating exception reports daily, as required by the ACP. We determined the content of the training met the intent of training because the DCAS Security Officers were now completing this monitor, which they were not during our prior audit. Because BEIS Office personnel completed the recommended action, this recommendation is closed. However, BEIS Office personnel could not demonstrate that these access controls were operating effectively because they did not have a repeatable process to review exception reports and identify all potential violations.

According to the NIST, organizations should employ an audit records control that contains information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome

of the event, and the identity of any individuals or subjects associated with the event.[30] Furthermore, the NIST states that achieving adequate information security requires, among other things:

- sound security practices that are well-documented and seamlessly integrated into the training requirements and daily routines of organizational personnel with security responsibilities; and
- continuous monitoring of organizations and information systems to determine the ongoing effectiveness of deployed security controls, changes in information systems and environments of operation, and compliance with legislation, directives, policies, and standards.

BEIS Office personnel walked us through one of the exception reports so we understood how personnel reviewed the reports, what BEIS Office personnel looked for, and what the BEIS Office personnel considered an anomaly. We determined that DCAS System Administrators did not conduct reviews with equal levels of scrutiny. For example, one reviewer did not report anomalies that another reviewer reported because the first reviewer was familiar with the DCAS staff. Additionally, the procedures used by the DCAS System Administrators to review the audit reports did not clearly define what a reportable anomaly was, and whether anomalies should be reported every time or only the first time identified. As a result, the BEIS Office personnel did not have assurance that the monitoring control was operating effectively. By having detailed, repeatable procedures, DCAS process owners and BEIS Office personnel would have greater assurance that this monitoring tool is effective and useful.

BEIS Office personnel provided the training that met the intent of our recommendation, which mitigated the control design deficiency. However, BEIS Office personnel could not demonstrate that these access controls were operating effectively because they did not have a consistent process to review the exception reports. BEIS Office personnel should refine, implement, and verify that the procedures for reviewing exception reports identify all exceptions that require followup or corrective actions.

Emergency Change Policies and Procedures

BEIS Office personnel improved the DCAS configuration management control over emergency change policies and ensured the control was designed effectively. This occurred because the BEIS Office personnel developed policies and procedures to identify emergency changes, how emergency changes should be handled, and the timeframe to implement emergency changes to ensure minimal impact to the

[30] NIST Special Publication 800-53 Rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013.

DCAS functionality. This action met the intent of Report No. DODIG-2017-015 Recommendation D.1.a.3 to develop and implement procedures to fix a critical system discrepancy, including the timeframes for resolving the discrepancy and clearly distinguishing between an emergency and urgent change. Because BEIS Office personnel completed the recommended action, this recommendation is closed. However, BEIS Office personnel were unable to demonstrate that these procedures were implemented and operating effectively because they have not completed any emergency changes since the development of the policies and procedures to verify their operating effectiveness.

During our prior audit, the DCAS Configuration Control Board charter defined an emergency change and stipulated that problem analysis, corrective action, and the release of the changes typically occur within 24 hours. However, the Master Software Development Plan did not identify procedures for implementing the Configuration Control Board policy. During our current audit, BEIS Office personnel provided a revised Master Software Development Plan, which included procedures necessary to implement the Configuration Control Board policy. According to these procedures, emergency changes should not require an estimate greater than 8 hours for development and testing to assist with the timeliness of completion. Approvals for these releases require only digitally signed e-mail approvals from DCAS Configuration Control Board members, the DCAS Software Engineering Branch Chief (or appointee), the DCAS System Manager (or appointee), and the DCAS Program Manager (or appointee).

BEIS Office personnel could not demonstrate that the configuration management control over emergency change policy was operating effectively because no emergency changes were required during the period of our review. BEIS Office personnel should review and verify that BEIS Office personnel execute and approve emergency changes in accordance with the Configuration Control Board charter and the DCAS Master Software Development Plan.

Conclusion on Design and Operation of Controls

BEIS Office personnel improved the operating effectiveness of controls because they developed, revised, disseminated, and implemented policies and procedures and trained personnel. As a result of the improved control operations, 15 of 20 recommendations can be closed. However, the recent implementation of actions to address 4 of the 15 closed recommendations did not provide BEIS Office and DFAS ESS personnel the opportunity to demonstrate or verify that these controls were operating effectively. Therefore, BEIS Office and DFAS ESS personnel need to perform procedures to verify that the controls they developed to address our recommendations are operating effectively to reduce the risk that DCAS may be vulnerable to inappropriate user access and critical system discrepancies.

Recommendations, Management Comments, and Our Response

Redirected Recommendation

As a result of management comments, we redirected Recommendation A.3 to the DISA Operations Center Financial Management Division Chief, who has the authority to implement the recommendation.

Recommendation A.1

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

a. Review and verify policies and procedures to execute periodic user reviews in accordance with the Defense Cash Accountability System Access Control Policy are operating effectively by documenting that 100 percent of sensitive users are reviewed each quarter and 100 percent of authorized users are reviewed within the last year.

Information and Technology, Defense Finance and Accounting Service Comments

The DFAS Information and Technology Director, responding for the DFAS BEIS and Other Systems Director, agreed with the recommendation. Specifically, the Information and Technology Director stated that training is provided quarterly to Information Owners, Information Owner Representatives, and Center Administrators to ensure reviewers thoroughly understand the DCAS ACP requirements for sensitive and authorized users reviews. The Information and Technology Director also stated that April 2018 testing on a recent quarterly review of sensitive user access controls showed that the control was operating effectively. Retesting of the annual review of authorized user access controls is scheduled for July 2018, and the estimated completion date is August 31, 2018.

Our Response

Comments from the Information and Technology Director addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved but will remain open. We will close the recommendation once we obtain documented access control results of the quarterly sensitive user reviews and the annual authorized user review and verify that these reviews captured 100 percent of DCAS users.

b. Review and verify that privileged user reviews are conducted within consistent timeframes from the end of each quarter.

Information and Technology, Defense Finance and Accounting Service Comments

The DFAS Information and Technology Director, responding for the DFAS BEIS and Other Systems Director, agreed with the recommendation, stating that the DCAS ACP will be revised to include a timeframe within which reviews should be completed. The Information and Technology Director also stated that the completion timeframe would be within 30 days of the last day of the current quarter. The estimated completion date is December 21, 2018.

Our Response

Comments from the Information and Technology Director addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved, but will remain open. We will close the recommendation once we obtain the updated DCAS ACP and verify that it includes review completion timeframes; and after we obtain results of the quarterly privileged user access reviews and verify that these reviews are performed within consistent timeframes from the end of each quarter.

c. Refine, implement, and verify the procedures for reviewing exception reports identify all exceptions that require followup or corrective actions.

Information and Technology, Defense Finance and Accounting Service Comments

The DFAS Information and Technology Director, responding for the DFAS BEIS and Other Systems Director, agreed with the recommendation. Specifically, the Information and Technology Director stated that the exception report has been reformatted and procedures will be more detailed to ensure reviews are performed consistently. The estimated completion date is December 21, 2018.

Our Response

Comments from the Information and Technology Director addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved, but will remain open. We acknowledge that the BEIS and Other Systems personnel reformatted the exception report to be more user-friendly. However, we will not close the recommendation until we obtain the reformatted exception reports and revised procedures and verify that the report consistently captures exceptions that require followup or corrective actions.

d. Review and verify policies and procedures to execute and approve emergency changes in accordance with the Configuration Control Board charter and the Defense Cash Accountability System Master Software Development Plan.

Information and Technology, Defense Finance and Accounting Service Comments

The DFAS Information and Technology Director, responding for the DFAS BEIS and Other Systems Director, agreed with the recommendation, stating that the DCAS System Master Software Development Plan was updated for emergency changes. The Information and Technology Director also stated that the Plan will again be updated with the emergency criteria cited in the Configuration Control Board charter. The estimated completion date is December 21, 2018.

Our Response

Comments from the Information and Technology Director addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved, but will remain open. We will close the recommendation once we obtain the updated DCAS System Master Software Development Plan and verify that it was updated to include both emergency changes and the emergency criteria cited in the Configuration Control Board charter.

Recommendation A.2

We recommend that the Revenue Branch Chief, Defense Working Capital Fund, Defense Information Systems Agency provide training to Defense Information Systems Agency Enterprise Services Directorate personnel on the requirements of the Defense Information Systems Agency's "Defense Working Capital Fund Service Level Agreement Guidance." This training should include annual Service Level Agreement review and documentation requirements.

Operations Center Financial Management Division, Defense Information Systems Agency

The DISA Operations Center Financial Management Division Chief, responding for the DISA Defense Working Capital Fund Revenue Branch Chief, agreed with the recommendation. Specifically, the Chief stated that annual training was provided to the Operations Center Financial Management Division personnel in November 2017, and the SLA procedures were reviewed. The Chief also stated that training will be provided annually, and actions to address the recommendation are completed.

Our Response

Comments from the Chief addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved but will remain open. We will close the recommendation once we obtain the SLA procedures on which training was provided and the current SLA and the prior SLA, and verify that the SLAs were reviewed and updated within 12 months of each other, as required by the Defense Working Capital Fund Service Level Agreement Guidance, including review and documentation requirements.

Recommendation A.3

We recommend that the Chief, Operations Center Financial Management Division, Defense Information Systems Agency, develop and implement procedures to ensure the Defense Information Systems Agency Customer Account Representative conducts annual Service Level Agreement reviews as required and document acknowledgment on the Service Level Agreement annual review table.

Operations Center Financial Management Division, Defense Information Systems Agency

The DISA Operations Center Financial Management Division Chief agreed with the recommendation, stating that the Customer Account Representative Desk Guide was revised to include procedures for reviewing and updating the SLA and completing the annual review. The Chief also stated that the Desk Guide was provided to the Defense Working Capital Fund Customer Management Branch personnel on April 30, 2018, and that all actions are completed.

Our Response

Comments from the Chief addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved but will remain open. We will close the recommendation once we: (1) obtain the current SLA and the prior SLA and verify that the SLAs were reviewed and updated within 12 months of each other, and (2) obtain the Customer Account Representative Desk Guide and any evidence to support its dissemination and verify that the Desk Guide was revised as stated.

Finding B

Several Application Level General Controls Need Improvement

Although BEIS Office personnel improved the operating effectiveness of controls in security management, access controls, configuration management, and contingency planning, 5 of 20 prior recommendations remain open. BEIS Office personnel need to coordinate with DFAS ESS personnel to make additional improvements to ISSO training certification, appropriate access authorization, Master Data Table and production changes, and contingency plan updates. Specifically, these recommendations remain open because:

- BEIS Office personnel did not require ISSOs to obtain and maintain DoD-required certifications (addressing Recommendation A.1.c.1);
- Authorizing officials did not ensure AMPS access requests matched the level of access users were assigned in DCAS, nor that users still required access (addressing Recommendation B.1.b);
- DFAS ESS personnel did not ensure the DCAS changes made by Table Administrators to the DCAS Master Data Tables were authorized, configured, and operated effectively (addressing Recommendation D.1.a.4);
- BEIS Office personnel did not clearly identify in the procedures how they validated that only authorized changes were made to the DCAS production environment[31] (addressing Recommendation D.1.a.2); and
- BEIS Office personnel did not coordinate with DISA to schedule and perform an annual test of the DCAS ISCP. (addressing Recommendation C.1.b)

As a result, selected controls were not working effectively to minimize the risk that users accessed DCAS without authorization or correct level of privileges. In addition, the control weaknesses identified could circumvent existing controls, which were operating as intended. Without proper controls over application level general 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 impair and diminish the DoD's ability to accomplish its mission. Consequently, the DoD could experience financial losses from expensive efforts to recover financial data, and DoD leadership's reliance on inaccurate or incomplete financial data processed to make critical decisions.

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

Additional Actions Needed to Close Application Level General Control Recommendations

Federal internal control standards state that a control cannot be effectively operating if it was not effectively designed and implemented.[32] Although BEIS Office personnel improved the operating effectiveness of controls in security management and configuration management, additional actions are needed. BEIS Office personnel need to require ISSOs to obtain and maintain DoD-required certifications, appropriately authorize DCAS access, and validate that only authorized system changes made to the DCAS production environment were approved. Additionally, DFAS ESS personnel need to verify, monitor, and track Master Data Table changes.[33] Therefore, the remaining 5 of our 20 recommendations cannot be closed until additional actions are completed. See Appendix B for the status of recommendations from Report No. DODIG-2017-015.

Information System Security Officer Certification

BEIS Office personnel did not require ISSOs to comply with the certification requirements established in DoD Manual 8570.01-M. This occurred because DFAS incorrectly concluded that ISSOs did not require DoD-required certifications even though the ISSOs perform four duties contained in DoD Manual 8570.01-M for an IA Technical Level I privileged user. Report No. DODIG-2017-015 Recommendation A.1.c.1 recommended the BEIS Office personnel to develop and implement procedures to require ISSOs to comply with the certification requirements established in DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Program." This recommendation will remain open until BEIS Office personnel demonstrate that the ISSOs obtained the applicable DoD-required certifications.

According to DoD Manual 8570.01-M, personnel performing certain identified functions, regardless of their occupational titles, must be identified as part of the Cybersecurity workforce and therefore must comply with corresponding certification requirements.[34] For example, the Manual identifies the function of applying appropriate computing environment access controls. DCAS ISSOs performed this function, as well as three additional functions identified by the

[32] GAO-14-704G, "Standards for Internal Control in the Federal Government," September 2014.

[33] Master Data Tables are sensitive data used to perform edits, verifications, and validations of data.

[34] The Cybersecurity workforce focuses on the operation and management of Cybersecurity capabilities for DoD systems and networks. Cybersecurity ensures that adequate security measures and established Cybersecurity policies and procedures as applied to all Information Systems and networks. The Cybersecurity workforce includes all privileged users and IA managers who perform any of the responsibilities or functions described in DoD Manual 8570.01-M.

Manual as part of the IA Technician Level I. DFAS agreed during our followup review that ISSOs belong in the Cybersecurity workforce, but stated that DFAS had incorrectly categorized individuals performing account management functions within DCAS as ISSOs.

According to DFAS, application account managers performed role assignments for non-privileged users, and did not themselves possess privileged access. DFAS stated that application account managers used a role within DCAS to assign roles, but these managers did not have the authority to grant privileged access. Additionally, application account managers did not grant access at the computing environment, network, or enclave levels. DFAS stated that application account managers were erroneously categorized as ISSOs, who should be part of the Cybersecurity workforce.

We determined DFAS incorrectly applied the requirements of the Manual, which dictates certification requirements based by functions performed. According to the DCAS ACP, ISSOs: (1) remove roles no longer required; (2) suspend and reinstate center users; and (3) assign roles, data sources, customers, organizations, or tables to center users. All of these functions are part of applying appropriate computing environment access controls, which the Manual identifies as a function requiring specialized certification. See Appendix C for additional information relating to these roles.

Furthermore, DFAS stated that the ISSOs did not grant access at the computing environment level. However, the Manual defines the computing environment as the local area network server host and its operating system, peripherals, and applications. DCAS is an application and is therefore part of the computing environment.

As a result, ISSOs did not obtain and maintain certifications required by the DoD to perform the functions identified in the Manual. Additionally, 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. Without a decision document from the DoD Chief Information Officer supporting DFAS's position that DCAS ISSOs do not require certifications under DoD Manual 8570.01-M, this recommendation cannot be closed. To meet the intent of Recommendation A.1.c.1, BEIS Office personnel should demonstrate that the ISSOs obtained the applicable DoD-required certifications.

Automated Authorizing Process for DCAS Users

BEIS Office personnel did not demonstrate that the DCAS access control over consistently authorizing the appropriate access to DCAS users was operating effectively. This occurred because authorizing officials, such as supervisors, Information Owners and their representatives, and Center Administrators, did not receive training to ensure that each user's SAAR for AMPS level of access request matched the user's granted level of DCAS access, or that the user still needed DCAS access. This action did not meet the intent of Report No. DODIG-2017-015 Recommendation B.1.b to train supervisors, Information Owners and their representatives, and Center Administrators to validate SAARs. SAAR validation efforts ensure that each SAAR is complete and requested access levels to perform sensitive activities are appropriate before signing the SAAR and authorizing each user account; therefore, this recommendation remains open. 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. To meet the intent of Recommendation B.1.b, BEIS Office personnel should demonstrate that supervisors, Information Owners and their representatives, and Center Administrators have been trained to ensure that requested access levels to perform sensitive activities are appropriate before approving the SAAR.

In October 2017, DFAS ESS personnel performed a detailed comparison of DCAS users at a role level and found 396 users whose current DCAS access did not match what was requested through AMPS.[35] This occurred because authorizing officials approved AMPS SAARs without ensuring the DCAS roles assigned to DCAS users were consistent with the requested AMPS SAARs roles for both sensitive and non-sensitive users. 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. Therefore, BEIS Office personnel should demonstrate that supervisors, Information Owners and their representatives, and Center Administrators have been trained to ensure that requested access levels to perform non-sensitive activities are appropriate before approving the SAAR and authorizing each user account.

[35] All access to functionality and data visibility is controlled through assigned (application, database, and system-level) roles based on DCAS responsibilities and duties.

Table Change Documentation

DFAS ESS personnel did not ensure the DCAS changes made by Table Administrators to the DCAS Master Data Tables were authorized, configured, and operated effectively. Although BEIS Office personnel developed procedures to verify DCAS Master Data Table changes, DFAS ESS personnel did not implement these procedures consistently. DFAS ESS personnel did not provide the required change request forms or supporting documentation, or both, for Master Data Table changes. As a result, this action did not meet the intent of Report No. DODIG-2017-015 Recommendation D.1.a.4 to develop and implement procedures to verify changes made by the Table Administrators to the DCAS Master Data Tables are authorized, tested, approved, monitored and tracked; therefore, this recommendation remains open.

The DCAS ACP requires DFAS ESS personnel to use a standard form to record Master Data Table changes. The DCAS Operating Guide instructs DFAS ESS personnel on how they should complete this form. The guide requires the DFAS ESS personnel to identify the table name, the change, effective date of change, and reason for the change. DFAS ESS personnel forward the completed form to the Table Administrator. According to the DCAS ACP, the Table Administrator makes the table change after obtaining the Table Administrator's supervisor's review and approval of a completed request along with supporting documentation.

DFAS ESS personnel walked us through four Master Data Table changes to explain the documentation available to identify the table name, the change, effective date of change, the reason for the change, and authorization for the change. After this walkthrough, we determined DFAS ESS personnel did not provide adequate support for any of the four Master Data Table changes. For example, DFAS ESS personnel did not provide the request form for one requested change. Additionally, DFAS ESS personnel provided documentation to support three table changes. However, these changes included table names that were not consistent between the requests and the Master Data Table list.

Based on the lack of adequate documentation, DFAS ESS personnel could not ensure that Table Administrators made the requested Master Data Table changes. Additionally, DFAS ESS personnel did not ensure the Table Administrator could restore DCAS to a previous version if the changes adversely impacted system functionality. In Report No. DODIG-2017-015, we directed Recommendation D.1.a.4 to BEIS Office personnel; however, based on the revised DCAS ACP, DFAS ESS personnel are now required to maintain responsibility for Master Data Table changes. Therefore, we will close Recommendation D.1.a.4 to the DFAS BEIS and Other Systems Director and redirect the recommendation to the DFAS Operations

Deputy Director. To meet the intent of the redirected recommendation, the DFAS Operations Deputy Director should verify changes made by the Table Administrators to the DCAS Master Data Tables are authorized, tested, approved, monitored, and tracked.

Production Changes

BEIS Office personnel did not demonstrate that the DCAS Configuration Management control over movement of programs and data among libraries was operating effectively. Although BEIS Office personnel developed and implemented the DCAS Audit Log Tracking Procedures, these procedures did not clearly identify how BEIS Office personnel validated that only approved changes were moved to the DCAS production environment. Additionally, the DCAS Audit Log Tracking Procedures did not clearly state how to verify that all configuration items were moved to the production environment.[36] As a result, this action did not meet the intent of Report No. DODIG-2017-015, Recommendation D.1.a.2 to validate that only authorized changes, including all configuration items, are approved and moved to the DCAS production environment; therefore, this recommendation remains open.

According to the NIST, one configuration change control step is for an organization to verify that they implemented the configuration change correctly.[37] BEIS Office personnel satisfied this requirement by developing and implementing the DCAS Audit Log Tracking Procedures. As part of these procedures, BEIS Office personnel are supposed to compare the Physical Configuration Audits and Schema Compare – Phase II reports to verify that only approved changes were implemented into production.[38] BEIS Office personnel provided and we reviewed nine configuration management audit reports. We identified discrepancies with all nine reports. For example,

- the DCAS Audit Log Tracking procedures identified configuration item types. However, these configuration item types were not identified in any of the nine Schema Compare – Phase II reports;
- the configuration item types did not correlate to the configuration item Categories in eight of the nine Schema Compare – Phase II reports; and
- all nine Physical Configuration Audits identified configuration item types that were not included in either the Audit Log Tracking Procedures or the Schema Compare – Phase II reports.

[36] Configuration item categories or types should be the same in the DCAS Audit Log Tracking Procedures and the Configuration Management Plan.

[37] NIST Special Publication 800-128, "Guide For Security-Focused Configuration Management Of Information Systems," August 2011.

[38] Physical configuration audits are designed to identify all configuration items associated with an approved change for release into the production environment. Schema Compare - Phase II reports are designed to compare the DCAS production environment after configuration changes were implemented to the system, and ensure that the production baseline was not modified in an unauthorized manner.

As a result of the identified discrepancies in all nine reports, BEIS Office personnel could not ensure that all authorized changes were implemented and no unauthorized changes or malicious code was placed into the production environment that could affect the functionality of the system.[39] To meet the intent of Recommendation D.1.a.2, BEIS Office personnel should validate that only authorized changes, including all configuration items, are approved and moved to the DCAS production environment. For example, BEIS Office personnel should reconcile the configuration item types from the Physical Configuration Audits to the Schema Compare – Phase II reports.

Contingency Plan Updates

BEIS Office personnel did not perform contingency plan updates. This occurred because BEIS Office personnel did not coordinate with DISA to ensure DCAS annual contingency plan testing was completed within one year from prior testing. As a result, BEIS Office personnel actions did not meet the intent of Report No. DODIG-2017-015 Recommendation C.1.b to incorporate lessons learned from the ISCP after action report into the DCAS ISCP in a timely manner; therefore, this recommendation remains open.

According to the NIST, Federal agencies must conduct periodic exercises or tests for their systems' contingency plans and incident response capabilities.[40] The DCAS SLA requires the Continuity of Operations Plan be exercised annually. During the audit, BEIS Office personnel participated in a test of the DCAS contingency plan review in September 2017. However, BEIS Office personnel did not comply with NIST, instead allowing a 19-month lag between that testing and the previous testing conducted in February 2016. Without completing testing once every 12 months, DFAS risks not being able to timely process more than 2 million monthly disbursement and collection transactions, which could negatively impact the DoD mission. Consequently, the DoD could experience financial losses from expensive efforts to recover financial data, and DoD leadership's reliance on inaccurate or incomplete financial data processed to make critical decisions. Additionally, control weaknesses could collectively impact financial statement audit readiness. To meet the intent of Recommendation C.1.b, BEIS Office personnel should coordinate with DISA to schedule and conduct the annual DCAS ISCP testing within a year of the prior testing.

[39] 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.

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

Conclusion on Open Prior Recommendations

BEIS Office personnel have improved 15 DCAS application level general controls since we issued Report No. DODIG-2017-015. However, five recommendations remain open. BEIS Office personnel should take additional actions to ensure DCAS performs as intended to support the DoD missions and minimize the risk that users inappropriately access DCAS. The control weaknesses identified could circumvent existing controls, which were operating as intended. For example, ineffective security management or access controls could negatively impact segregation of duty controls, which were independently operating as intended during our prior audit. Because of these control weaknesses, DCAS is vulnerable to availability interruptions and lost or incorrectly processed data.

Recommendations, Management Comments, and Our Response

Recommendation B.1

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

a. Monitor the status of the four open recommendations that remain directed to the Director, Business Enterprise Information Services and Other Systems and expedite the corrective actions necessary to close those recommendations.

Information and Technology, Defense Finance and Accounting Service, and Enterprise Solutions and Standards, Defense Finance and Accounting Service Comments

The DFAS Information and Technology Director and the DFAS ESS Director, responding for the DFAS BEIS and Other Systems Director, partially agreed with the recommendation. Comments provided for each of the four open recommendations from the prior report and our responses follow. See Appendix B for recommendation details.

DODIG-2017-015 Recommendation A.1.c.1: The DFAS Information and Technology Director, responding for the DFAS BEIS and Other Systems Director, disagreed with the recommendation to monitor the status of and expedite corrective actions for an open recommendation requiring ISSOs to comply with the certification requirements established in DoD Manual 8570.01-M. The Information and Technology Director also disagreed that personnel performing account management functions require cybersecurity certification. The Information and Technology Director stated that the account managers have

limited access to create, maintain and remove authorized access for pre-established roles within the system. Furthermore, the Information and Technology Director stated that application account managers do not require access to the computing environment, network, or enclave to perform role assignments for non-privileged users. The Information and Technology Director stated that personnel in this role were erroneously included in the DoD Chief Information Office Cybersecurity Strategy Workforce, of which personnel must have cybersecurity certification. According to the Information and Technology Director, the DoD Chief Information Office Cybersecurity Strategy, Policy, and Workforce personnel stated that personnel who only establish accounts for other users to get access, and who have no administrative privileged user rights beyond account enrolling and removing, should not be considered Cybersecurity users and no waiver is needed to exclude these personnel from the Cybersecurity workforce.

Our Response

Comments from the Information and Technology Director did not address all the specifics of the recommendation; therefore, the recommendation is unresolved and will remain open. We disagree that the account managers are not privileged users because our analysis identified that the ISSOs were included in the privileged access user reviews performed by DFAS. As stated within Finding B, the DCAS ACP states that ISSOs perform some of the duties identified in DoD Manual 8570.01-M that require cybersecurity certification. Moreover, the ISSO duties defined in the DCAS ACP have not changed since our original recommendation, and the Information and Technology Director agreed with that recommendation. We request that the DFAS BEIS and Other Systems Director respond to the final report and include the ISSOs cybersecurity certifications or provide a decision document from the DoD Chief Information Officer supporting the DFAS position that DCAS ISSOs do not require cybersecurity certifications as required by DoD Manual 8570.01-M.

DODIG-2017-015 Recommendation B.1.b: The DFAS ESS Director, responding for the DFAS BEIS and Other Systems Director, agreed with the recommendation, stating that DCAS training is conducted quarterly to ensure Information Owners, Representatives, and Center Administrators thoroughly understand the DCAS ACP procedures when approving non-sensitive user accounts. The ESS Director also stated that this recommendation resulted not from identified inappropriate access, but because we only reviewed a single review period. Additionally, the ESS

Director stated that the access control was fully tested during the Statement on Standards for Attestation Engagements No. 18 engagement, and DFAS received no recommendations in the report provided.[41] The ESS Director stated that all actions to address this recommendation were completed in November 2017.

Our Response

Comments from the ESS Director addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved, but will remain open. We agree that the ESS Director provided the independent engagement report and that no recommendations in this area were provided to DFAS. However, the report did identify exceptions with 10 of 91 SAARs. Specifically, the ISSOs did not approve the SAARs, as required by DFAS policy. We will close the recommendation once we receive documentation verifying that supervisors, Information Owners and their representatives, and Center Administrators approve each user's SAAR and authorize the user account with access levels necessary to perform sensitive activities required by job duties.

DODIG-2017-015 Recommendation D.1.a.2: The DFAS Information and Technology Director, responding for the DFAS BEIS and Other Systems Director, agreed with the recommendation to validate that only authorized changes were made to the DCAS production environment, stating that a new automated process was implemented in January 2018. Additionally, the Information and Technology Director stated that the Information and Technology personnel are testing the automated process and validating its consistency, and will create new procedures for the process. The estimated completion date is December 21, 2018.

Our Response

Comments from the Information and Technology Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once we obtain and verify that the new procedures include repeatable processes for validating that only authorized changes were made to the DCAS production environment.

DODIG-2017-015 Recommendation C.1.b: The DFAS Information and Technology Director, responding for the DFAS BEIS and Other Systems Director, agreed with the recommendation, stating that contingency plan testing is scheduled for fourth quarter FY 2018. The estimated completion date is December 21, 2018.

[41] As conducted by independent service auditor KPMG LLP and reported in the Service Organization Controls Report (SOC1), "Report on the Defense Finance and Accounting Service Transaction Distribution Service's Description of its System Supporting the Delivery of Transaction Distribution Services Provided by DFAS and the Suitability of the Design and Operating Effectiveness of Its Controls, For the Period of October 2016 to June 30, 2017" on August 15, 2017.

Our Response

Comments from the Information and Technology Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendations once we obtain the results of the fourth quarter FY 2018 DCAS contingency plan testing and verify that BEIS Office personnel incorporated the lessons learned from the DCAS contingency plan after action report.

b. Demonstrate that supervisors, Information Owners and their representatives, and Center Administrators have been trained to ensure that requested access levels to perform non-sensitive activities are appropriate before approving the System Authorization Access Request and authorizing each user account.

Enterprise Solutions and Standards, Defense Finance and Accounting Service Comments

The DFAS ESS Director, responding for the DFAS BEIS and Other Systems Director, agreed with the recommendation, stating that DCAS training is conducted quarterly to ensure Information Owners, Representatives, and Center Administrators thoroughly understand the DCAS ACP procedures when approving non-sensitive user accounts. The ESS Director also stated that this recommendation resulted not from identified inappropriate access, but because the audit team reviewed only a single review period. Additionally, the ESS Director stated that the access control was fully tested during the Statement on Standards for Attestation Engagements No. 18 engagement, and DFAS received no recommendations in the report provided. The ESS Director stated that all actions to address this recommendation were completed in November 2017.

Our Response

Comments from the ESS Director addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved, but will remain open. We acknowledge that the ESS Director provided the independent engagement report and that no recommendations in this area were provided to DFAS. However, the report identified exceptions with 10 of 91 SAARs. Specifically, the ISSOs did not approve the SAARs, as required by DFAS policy. We will close the recommendation once we receive documentation verifying that supervisors, Information Owners and their representatives, and Center Administrators approve each user's SAAR and authorize the user account with access levels necessary to perform sensitive activities and appropriate to perform non-sensitive activities, as required by job duties.

c. Coordinate with the Defense Information Systems Agency to conduct the annual Defense Cash Accountability System Information System Contingency Plan testing within a year of the prior testing.

Information and Technology, Defense Finance and Accounting Service Comments

The DFAS Information and Technology Director, responding for the DFAS BEIS and Other Systems Director, agreed with the recommendation. The Information and Technology Director stated that the DCAS contingency of operations policy testing was rescheduled to accommodate a tabletop exercise, with an estimated completion date of December 21, 2018.

Our Response

Comments from the Information and Technology Director addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved, but will remain open. We will close the recommendation once we obtain documented results from the rescheduled annual DCAS Information System Contingency Plan and verify it was tested within 1 year of the prior test.

Recommendation B.2

We recommend that the Deputy Director, Operations, Defense Finance and Accounting Service, verify changes made by the Table Administrators to the Defense Cash Accountability System Master Data Tables are authorized, tested, approved, monitored, and tracked.

Enterprise Solutions and Standards, Defense Finance and Accounting Service Comments

The DFAS ESS Director, responding for the DFAS BEIS and Other Systems Director, agreed with the recommendation, stating that the DCAS Program Management Office implemented process improvements to address the recommendation. The ESS Director stated that one improvement included creating standardized procedures that use documentation allowing supervisors instead of the DFAS Operations Deputy Director to authorize each table update. Additionally, the DCAS Program Management Office personnel implemented a system change to generate a daily report showing table updates performed by each user. Finally, the DCAS Program Management Office personnel provided training on this new process to all users. The ESS Director stated that the DCAS Program Management Office personnel tested the controls around this recommendation in October 2017 and passed on all samples tested. The ESS Director stated that all actions to address this recommendation were completed in December 2017.

Our Response

Comments from the ESS Director addressed all specifics of the recommendation, and no further comments are required. Therefore, the recommendation is resolved, but will remain open. We acknowledge that the ESS Director provided evidence of the recently implemented process improvements. Specifically, the ESS Director provided an example of the report that is generated daily to show table updates performed by each user. The ESS Director also provided a blank DCAS Table Update Request Form, which requires approval routing to the supervisor. However, we require additional documentation to satisfy the recommendation. We will close the recommendation once we: (1) obtain the query logic used to run the daily table updates report; (2) obtain completed DCAS Table Update Request Form packages; (3) obtain evidence of monitoring table updates according to procedures; and (4) verify that the changes made by the Table Administrator to the DCAS Master Data Table are authorized, tested, approved, monitored, and tracked.

Appendix A

Scope and Methodology

We conducted this FISCAM audit from May 2017 through April 2018 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 Government Accountability Office FISCAM, February 2009, to develop the procedures performed during this audit. Our review focused on the application level general controls as defined by FISCAM and the control deficiencies identified in our prior audit report, Report No. DODIG-2017-015.[42] Based on availability and timing, we reviewed the first, second, and third quarters of FY 2017 documentation. To understand the updates and changes made to improve the DCAS control environment, we reviewed:

- DCAS ACP;
- ISSO appointment letters;
- DCAS SLA;
- DCAS SAARs and SAAR audit logs;
- DCAS Information System Contingency Plan;
- DCAS Configuration Management Plan;
- DCAS Master Software Development Plan;
- DCAS Master Data and DCAS Master Data Table changes;
- DCAS Testing Management Plan;
- DCAS Configuration Control Board Charter;
- DCAS Incidence Response Reporting Exercise After Action Report;
- DCAS-generated listings, logs, and reports; and
- DCAS system documentation, policies, and procedures.

We compared the documentation above to NIST, DoD, and DFAS requirements. Furthermore, we interviewed applicable DFAS personnel and followed up on the responses with interviews and documentation requests.

We interviewed applicable DISA personnel regarding SLAs and applicable DISA guidance.

[42] 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.

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, 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.

Prior Coverage

During the last 5 years, the DoD Office of Inspector General (DoD OIG) issued one report discussing DCAS application level general controls. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/.

DoD OIG

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

> This audit report objective was to determine whether the process used by the Department of the Navy to reconcile its Fund Balance With Treasury Account was effective. The DoD OIG found that the Department of the Navy may have used unreliable computer-processed data because DCAS and the Program Budget Information System had significant control deficiencies identified during FISCAM testing. In addition, the Department of the Navy did not identify compensating controls to ensure the reliability of the data.

Appendix B

Summary of Prior Recommendations and Current Status

We issued 20 recommendations in Report No. DODIG-2017-15, "Application Level General Controls for the Defense Cash Accountability System Need Improvement," November 10, 2016, related to four application level general control categories. As summarized in Appendix B, we have verified that DFAS implemented corrective actions to support closing 15 of the 20 recommendations.

Application Level General Controls Category	Prior Recommendation	DFAS-Identified Completion Date Per Management Comments Dated 19 JAN 2017	Current DoD OIG Conclusions (Finding)
Security Management	**A.1.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.	10/31/2016	Closed
Security Management	**A.1.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.	10/31/2016	Closed
Security Management	**A.1.c.1** – Develop and implement procedures to require Information System Security Officers to comply with the certification requirements established in DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Program."	1/31/2017	**Open (Finding B)**
Security Management	**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."	Completed	Closed

Summary of Prior Recommendations and Current Status (cont'd)

Application Level General Controls Category	Prior Recommendation	DFAS-Identified Completion Date Per Management Comments Dated 19 JAN 2017	Current DoD OIG Conclusions (Finding)
Security Management	**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.	Completed	Closed
Access Controls	**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.	10/31/2016	Closed
Access Controls	**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.	10/31/2016	**Open (Finding B)**
Access Controls	**B.1.c** – Train Defense Cash Accountability System IA 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.	Completed	Closed
Access Controls	**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.	Completed	Closed
Access Controls	**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.	Completed	Closed
Access Controls	**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.	Completed	Closed

Summary of Prior Recommendations and Current Status (cont'd)

Application Level General Controls Category	Prior Recommendation	DFAS-Identified Completion Date Per Management Comments Dated 19 JAN 2017	Current DoD OIG Conclusions (Finding)
Access Controls	**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.	10/31/2016	Closed
Contingency Planning	**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.	1/31/2017	Closed
Contingency Planning	**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.	Completed	**Open (Finding B)**
Configuration Management	**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.	10/31/2016	Closed
Configuration Management	**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.	Completed	**Open (Finding B)**
Configuration Management	**D.1.a.3** – Develop and implement procedures to 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.	1/31/2017	Closed

Summary of Prior Recommendations and Current Status (cont'd)

Application Level General Controls Category	Prior Recommendation	DFAS-Identified Completion Date Per Management Comments Dated 19 JAN 2017	Current DoD OIG Conclusions (Finding)
Configuration Management	**D.1.a.4** – Develop and implement procedures to 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.	Completed	**Redirected (Finding B)**
Configuration Management	**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.	Completed	Closed
Configuration Management	**D.1.c** – Train applicable BEIS Office personnel on Vulnerability Management Plan responsibilities.	Completed	Closed

Appendix C

Information System Security Manager and Information System Security Officers

The ISSM is a DoD-defined role. The ISSM serves as a principal advisor on all matters, technical or otherwise, involving information system security. These duties are carried out in close collaboration with the information system owner. Specifically, the ISSM in the DoD is charged with the following responsibilities related to authorizing or managing information system access:

- Develop and maintain a system-level IA program, identifying the IA architecture, requirements, objectives and policies; IA personnel; and IA policies and procedures.
- Ensure information ownership or stewardship, or both, responsibilities are established for each DoD information system, including accountability, access approvals, and special handling requirements.
- Ensure ISSO appointment is in writing when one or more ISSOs are required to assist the ISSM in carrying out his or her responsibilities. When circumstances warrant, a U.S. citizen may fill both ISSM and ISSO roles.
- Maintain oversight for all privileged user assignments to ensure separation of functions and compliance with personnel security criteria established in DoD 5200.2-R.[43]
- When no ISSO is assigned to assist with access review processing, ensure users have the requisite security clearance or access authorization (Information Technology Level), or both, and are aware of their IA responsibilities before granting access to the information system—a responsibility typically assigned to the ISSO.

The DoD regards the ISSO as an assistant to the ISSM, with the ISSM operating in an oversight role. The ISSO is assigned the same responsibilities as the ISSM, and DoD instructions make the ISSO accountable to the ISSM. When the ISSO performs access authorization and management, the ISSO is responsible for ensuring users have requisite security clearances or access authorization, or both, and are aware of their IA responsibilities before receiving access to the information system.

In DFAS, an Administrative ISSO is a DFAS-defined role performing specified IA-related duties, including reviewing and signing access request forms, resetting user passwords, and conducting reviews to validate user access of respective

[43] This DoD regulation has been rescinded and replaced with DoD Manual 5200.2, "Procedures for the DoD Personnel Security Program (PSP)", April 3, 2017

systems at least annually. As long as Administrative ISSO system access is limited to resetting passwords, with no additional privileged access (for example, cannot create user accounts or modify user roles), they are not considered privileged users for the purposes of IA workforce classification and are not required to obtain an IA certification otherwise required by DoD Manual 8570.01-M.[44] For DCAS, Center Administrators are Administrative ISSOs.

DFAS has identified System Administrators and System Security Officers as privileged users. They are appointed as Application ISSOs and assist the ISSM and ISSO, as required, in implementing the IA program for the system. In regard to access controls, they establish and manage authorized user accounts for DoD information systems. This would include configuring access controls to enable access to authorized information and removing authorizations when access is no longer needed.

[44] DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, incorporating changes dated November 10, 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 June 1, 2018

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Draft Report Followup Audit: Application Level General Controls for the Defense Cash Accountability System Project No. D2017-D000FL-0141.000

We concur with recommendations A.1.a, A.1.b, A.1.c, A.1.d, B.1.c and B.1.b, C.1.b, D.1.a.2 and D.1.a.4 listed under recommendation B.1.a.

We do not concur with A.1.c.1 under recommendation B.1.a. DFAS disagrees that personnel performing account management functions require a cybersecurity certification. DFAS partitioned account management functions into a role separate from privileged system administration functions.

Request closure of B.1.b and B.2 for the current audit and B.1.b and D.1.a.4 for the previous audit "Application Level General Controls for the Defense Cash Accountability System (DCAS) Need Improvement" Report No. DoDIG-2017-015.

Management comments with estimated completion dates and supporting documentation are attached.

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

GILLISON.AARON.P[redacted]
ETER[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)

Followup Audit: Application Level General Controls for the Defense Cash Accountability System
Project No. D2017-D000FL-0141.000

Recommendation A.1

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

Recommendation A.1.a.: Review and verify policies and procedures to execute periodic user reviews in accordance with the Defense Cash Accountability System Access Control Policy are operating effectively by documenting that 100 percent of sensitive users are reviewed each quarter and 100 percent of authorized users are reviewed within the last year.

Management Response: The Defense Cash Accountability System (DCAS) Access Control Policy (ACP) states Information Owners, Representatives and Center Administrators ensure the appropriateness for each DCAS role assigned. It further states quarterly access reviews are required 100% for sensitive users and annually for authorized users. Quarterly DCAS trainings are consistently held to ensure Information Owners, Representatives and Center Administrators fully understand the access control policy guideline when access reviews are performed. These access controls are designed effectively and a recent quarterly review of DCAS access control for sensitive users was fully tested with FISCAM Control AS-2.6.2 in April of 2018 and shows the controls are operating effectively. Control operating effectiveness of authorized users annual review will be re-tested under AS-2.4.2 in July 2018.
Estimated Completion Date (ECD): August 31, 2018

Recommendation A.1.b: Review and verify that privileged user reviews are conducted within consistent timeframes from the end of each quarter.

Management Response: The privileged user reviews are conducted quarterly. The next version of the ACP will include a timeframe to complete the reviews after the last day of the current quarter, within 30 days. During FY17 and first quarter FY18, DCAS only had one Information System Security Manager working on three systems to complete Risk Management Framework (RMF). Due to limited resources in FY17, some of the reviews took longer which caused inconsistent timeframes. **ECD: December 21, 2018**

Recommendation A.1.c.: Refine, implement, and verify the procedures for reviewing exception reports identify all exceptions that require follow-up or corrective actions.

Management Response: Application Violations & Exceptions Report has been reformatted for an easier understanding and a more detailed procedure will ensure reviews are being conducted consistently across the team reviewing them. **ECD: December 21, 2018**

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

Recommendation A.1.d: Review and verify policies and procedures to execute and approve emergency changes in accordance with the Configuration Control Board charter and the Defense Cash Accountability System Master Software Development Plan.

Management Response: The DCAS System Master Software Development Plan has been updated for emergency changes and will be updated again with the emergency criteria cited in the Configuration Control Board (CCB) charter. **ECD: December 21, 2018**

Recommendation B.1

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

Recommendation B.1a: Monitor the status of the four open recommendations that remain directed to the Director, Business Enterprise Information Services and Other Systems and expedite the corrective actions necessary to close those recommendations.

Recommendation: BEIS Office personnel did not require ISSOs to obtain and maintain DoD required certifications (addressing Recommendation A.1.c.1 from previous audit DoD-2017-015, Project No. D000FS-0066.000).
Management Response: DFAS disagrees that personnel performing account management functions require a cybersecurity certification. DFAS partitioned account management functions into a role separate from privileged system administration functions. These account managers have very limited access to create, maintain and remove authorized access for pre-established roles within the system. Application account managers perform role assignments for non-privileged users only. They use a role within the application to perform this function and do not require access to the computing environment, network or enclave to do so. They do not possess privileged access, nor are they able to grant privileged access. They do not grant access at the computing environment, network or enclave level. As such, we determined, through policy research, consultation with other DoD Services and Agencies and confirmation with the DoD CIO Cybersecurity Strategy, Policy, and Workforce, that these personnel were erroneously included in the CS workforce. The minimal duties assigned to these employees present a low risk to the agency and may be effectively managed without requiring an unnecessary certification. DFAS reached out to the DoD CIO Cybersecurity Strategy, Policy, and Workforce regarding exclusion of Operations employees from the Cybersecurity Workforce. They responded, "Our guidance is that if the personnel simply establish accounts for other users to get access to the enterprise applications, and have no sys admin privileged user rights beyond account enrolling / de-enrolling, then they should not be considered Cyber Security users. No waiver is needed to exclude these personnel from the CS workforce."

Recommendation: Authorizing officials did not ensure AMPS access requests matched the level of access users were assigned in DCAS, nor that users still required access (addressing Recommendation B.1.b from previous audit DoD-2017-015, Project No. D000FS-0066.000).
Management Response: Enterprise Solutions and Standards (ESS) provided response in recommendation B.1.b below.

Recommendation: DFAS ESS personnel did not ensure the DCAS changes made by Table Administrators to the DCAS Master Data Tables were authorized, configured, and operated effectively (addressing Recommendation D.1.a.4 from previous audit DoD-2017-015, Project No. D000FS-0066.000)

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

Management Response: ESS provided response in recommendations B.2 below.

Recommendation: BEIS Office personnel did not clearly identify in the procedures how they validated that only authorized changes were made to the DCAS production environment30 (addressing Recommendation D.1.a.2 from previous audit DoD-2017-015, Project No. D000FS-0066.000).

Management Response: A new automated process has been implemented in January 2018. IT is currently in the testing phase and validating consistency with the process. IT will develop a new procedure for this new process. **ECD: December 21, 2018**

Recommendation: BEIS Office personnel did not coordinate with DISA to schedule and perform an annual test of the DCAS ISCP (addressing Recommendation C.1.b from previous audit DoD-2017-015, Project No. D000FS-0066.000).

Management Response: COOP testing has been scheduled for fourth quarter FY18. Evidence was provided that DISA had scheduling issues in FY17. See response to B.1.c below.
ECD: December 21, 2018

Recommendation B.1.b: Demonstrate that supervisors, Information Owners and their representatives, and Center Administrators have been trained to ensure that requested access levels to perform non-sensitive activities are appropriate before approving the System Authorization Access Request and authorizing each user account.

Management Response: The DCAS ACP states Information Owners, Representatives and Center Administrators ensure the appropriateness for each DCAS role assigned. It further states that non-sensitive end users require annual review while sensitive end users are performed quarterly. Quarterly DCAS trainings are performed to ensure Information Owners, Representatives and Center Administrators fully understand the access control policy guideline when approving non-sensitive end users. DODIG performed testing for a single quarterly access review period. They found no findings of inappropriate access; however, they could not close this finding because they did not perform a full annual review. A review of DCAS access control was fully tested with the SSAE18 engagement and received no recommendations. **Completion Date: November 2017**

Recommendation B.1.c: Coordinate with the Defense Information Systems Agency to conduct the annual Defense Cash Accountability System Information System Contingency Plan testing within a year of the prior testing.

Management Response: DCAS requested a full simulation COOP instead of a Tabletop Exercise in FY17. However, because DCAS was on a virtual test server it was determined it was not big enough to handle the data that our production server contains, and therefore the DCAS COOP was rescheduled to accommodate a tabletop instead. **ECD: December 21, 2018**

Recommendation B.2

We recommend that the Deputy Director, Operations, Defense Finance and Accounting Service, verify changes made by the Table Administrators to the Defense Cash Accountability System Master Data Tables are authorized, tested, approved, monitored, and tracked.

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

Management Response: DCAS PMO has implemented the following process improvements to address this finding. First, the DCAS PMO created standardized procedures utilizing documentation allowing supervisors to sign off on each table update in lieu of the Deputy Director, Operations, Defense Finance and Accounting Service. Second, a System Change (X2953 - MISSING I&T MASTER TABLE CHANGE MONITORING REPORTS OR LOGS) was implemented in DCAS to produce a daily report of the table updates performed by each user. Finally, the DCAS PMO facilitated three training sessions to provide this new process to all users. The controls around this recommendation were recently tested by DCAS PMO under FISCAM BP 4.4.2 in October 2017 and passed on all samples tested.
Completion Date: December 2017

Enterprise Solutions and Standards, Defense Finance and Accounting Service

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

MEMORANDUM FOR DIRECTOR, INFORMATION & TECHNOLOGY, AUDIT SUPPORT

SUBJECT: Management Comments to Draft Report, Follow-up Audit: Application Level General Controls for the Defense Cash Accountability System, D2017-D000FL-0141.000, dated April 25, 2018

Attached are management comments for subject audit recommendations B.1.b and B.2.

My point of contact for additional information is [redacted]. [redacted] can be reached at [redacted].

KNIGHT.EDNA.JO[redacted]

Edna J. Knight
Director, Enterprise Solutions & Standards

Attachment:
As stated

www.dfas.mil

Enterprise Solutions and Standards, Defense Finance and Accounting Service (cont'd)

Management Comments to DODIG Draft Report, Follow-up Audit: Application Level General Controls for the Defense Cash Accountability System, D2017-D000FL-0141.000, dated April 25, 2018

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

Recommendation B.1.b. Demonstrate that supervisors, Information Owners and their representatives, and Central Administrators have been trained to ensure that requested access levels to perform non-sensitive activities are appropriate before approving the System Authorization Access Request and authorizing each user account.

Management Comments. The DCAS Access Control Policy states Information Owners, Representatives and Center Administrators ensure the appropriateness for each DCAS role assigned. It further states that non-sensitive end users require annual review while sensitive end users are performed quarterly. Quarterly DCAS trainings are performed to ensure Information Owners, Representatives and Center Administrators fully understand the access control policy guideline when approving non-sensitive end users. DODIG performed testing for a single quarterly access review period. They found no findings of inappropriate access however they could not close this finding because they did not perform a full annual review. A review of DCAS access control was fully tested with the SSAE18 engagement and received no recommendations.

Completed Date. November 2017

Recommendation B.2. We recommend that the Deputy Director, Operations, Defense Finance and Accounting Service, verify changes made by the Table Administrators to the Defense Cash Accountability System Master Data Tables are authorized, tested, approved, monitored and tracked.

Management Comments. DCAS PMO has implemented the following process improvements to address this finding. First, the DCAS PMO created standardized procedures utilizing documentation allowing supervisors to sign off on each table update in lieu of the Deputy Director, Operations, Defense Finance and Accounting Service.

Second, a System Change (X2953 - MISSING I&T MASTER TABLE CHANGE MONITORING REPORTS OR LOGS) was implemented in DCAS to produce a daily report of the table updates performed by each user.

2

Enterprise Solutions and Standards, Defense Finance and Accounting Service (cont'd)

Finally, the DCAS PMO facilitated three training sessions to provide this new process to all users. The controls around this recommendation were recently tested by DCAS PMO under FISCAM BP 4.4.2 in October 2017 and passed on all samples tested.

Completed Date. December 2017

3

Operations Center Financial Management Division, Defense Information Systems Agency

Final Report Reference

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

30 May 2018

MEMORANDUM FOR DOD INSPECTOR GENERAL

SUBJECT: Follow-up Audit: Application Level General Controls for the Defense Cash Accountability System, D2017-D000FL-0141.000

Reference: DODIG Draft Report, Follow-up Audit: Application Level General Controls Defense Cash Accountability System, D2017-D000FL-0141.000, 25 April 2018.

1. The following comments depict our position regarding the DODIG Draft Report:

   a. Recommendation A.2 – Concur

      (1) Provide training to Defense Information Systems Agency Enterprise Services Directorate personnel on the requirements of Defense Information Systems Agency's "Defense Working Capital Fund Service Level Agreement Guidance." This training should include annual Service Level Agreement review and documentation requirements.

      (2) Action: Complete

      (3) Annual training is held with the OCF staff. In November 2017, annual training was provided to the OCF staff and the SLA procedures were reviewed. Training will be given annually.

   b. Recommendation A.3 – Concur

      Redirected Recommendation A.3

      (1) Develop and implement procedures to ensure the Defense Information Systems Agency Customer Account Representative conducts annual Service Level Agreement reviews as required and document acknowledgment on the Service Level Agreement annual review table.

      (2) Action: Complete

      (3) The Customer Account Representative Desk Guide was updated and published/ distributed to the OCF4 staff on April 30. This document was updated to reflect the steps to take for reviewing/updating the SLA and completing the annual review. The Customer Account Representative Desk Guide will be reviewed annually and updated if required.

Operations Center Financial Management Division, Defense Information Systems Agency (cont'd)

DISA MEMO, OCF, Follow-up Audit: Application Level General Controls for the Defense Cash Accountability System, D2017-D000FL-0141.000

2. Please feel free to contact me at [redacted] or via email: [redacted] should you have any questions.

BYRON Z. STEPHENSON
Chief, Operations Center Financial
Management Division

2

Acronyms and Abbreviations

ACP	Access Control Policy
AMPS	Accounts Management and Provisioning System
BEIS	Business Enterprise Information Services
DCAS	Defense Cash Accountability System
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
ESS	Enterprise Shared Services
FISCAM	Federal Information System Controls Audit Manual
IA	Information Assurance
ISCP	Information System Contingency Plan
ISSM	Information System Security Manager
ISSO	Information System Security Officer
NIST	National Institute of Standards and Technology
SAAR	System Authorization Access Request
SLA	Service Level Agreement


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

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/Components/Administrative-Investigations/DoD-Hotline/.

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

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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