Report No. DODIG-2012-118 August 14, 2012

Inspector General
United States Department of Defense

Defense Finance and Accounting Service Needs to Strengthen Procedures to Comply with the Federal Financial Management Improvement Act

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
14 AUG 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Finance and Accounting Service Needs to Strengthen Procedures to Comply with the Federal Financial Management Improvement Act	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense Office of Inspector General,4800 Mark Center Drive,Alexandria,VA,22350-1500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**30**	

Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit at auditnet@dodig.mil.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing auditnet@dodig.mil, or by mail:

Department of Defense Office of Inspector General
Office of the Deputy Inspector General for Auditing
ATTN: Audit Suggestions/13F25-04
4800 Mark Center Drive
Alexandria, VA 22350-1500

Acronyms and Abbreviations

DCPS	Defense Civilian and Pay System
DFAS	Defense Finance and Accounting Service
FFMIA	Federal Financial Management Improvement Act
GSA	General Services Administration
IG	Inspector General
I&T	Information and Technology
MOA	Memorandum of Agreement
OIG	Office of Inspector General
PIO	Performance Improvement Opportunity
PKI	Public Key Infrastructure
SAS 70	Statement of Auditing Standards Number 70

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

August 14, 2012

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Defense Finance and Accounting Service Needs to Strengthen Procedures to Comply with the Federal Financial Management Improvement Act (Report No. D-2012-118)

We are providing this report for your information and use. The Defense Finance and Accounting Service needs to assess the Defense Civilian Pay System's compliance with applicable Federal Financial Management Improvement Act requirements and secure access to two payroll offices at Indianapolis, Indiana, that process sensitive payroll information.

We considered management comments provided by the Director, Information and Technology on behalf of the Director, Defense Finance and Accounting Service on the draft of this report when preparing the final report. The Director, Information and Technology comments conformed to the requirements of DoD Directive 7650.3; therefore, additional comments are not required.

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 601-5945 (DSN 329-5945).

Lorin T. Venable

Lorin T. Venable, CPA
Acting Assistant Inspector General
DoD Payments and Accounting Operations

Results in Brief: Defense Finance and Accounting Service Needs to Strengthen Procedures to Comply with the Federal Financial Management Improvement Act

What We Did

We determined whether physical security over Defense Civilian Pay System (DCPS) data was adequate and whether DCPS complied with the requirements of the Federal Financial Management Improvement Act (FFMIA).

What We Found

The Defense Finance and Accounting Service (DFAS) did not perform annual or complete self-assessments on DCPS to determine FFMIA compliance and did not develop a remediation plan to address requirements that DCPS did not meet. This occurred because DFAS officials were waiting on additional DoD guidance before pursuing FFMIA compliance further. Systems that do not comply with FFMIA requirements restrict the ability of organizations to consistently and accurately record the assets, liabilities, revenues, expenses, and the full costs of programs and activities of the Federal Government.

DFAS Officials did not secure two of four Civilian Pay Operations locations at Indianapolis with cipher locks. This occurred because DFAS had not completed required actions with the General Services Administration to secure the locations. Without adequate controls over physical access, individuals could gain unauthorized access to computers and sensitive payroll data contained in online files and hardcopy printouts.

During the audit, DFAS Indianapolis funded a new access control project that will establish lockable space and eliminate access concerns. DFAS Indianapolis expected to complete the project by the end of FY 2012.

What We Recommend

We recommend the Director, DFAS, consult the "DFAS Financial Management Systems Requirements Manual" to:

- identify the requirements that apply to DCPS,
- determine which ones DCPS cannot perform, and
- develop a remediation plan to address deficiencies.

Management Comments and Our Response

The Director, Information and Technology responded for the Director, DFAS. He concurred and stated that the DCPS system/functional managers will conduct a self-assessment and identify applicable requirements. If the self-assessment finds DCPS not compliant, the system manager will identify required corrective actions and develop a remediation plan to bring DCPS into substantial compliance. The Director, Information and Technology, comments were responsive and no additional comments are required. Please see the recommendations table on the back of this page.

Recommendations Table

Management	Recommendations Require Comment	No Additional Comments Required
Director, Defense Finance and Accounting Service		A.1.a, A.1.b, A.2

Table of Contents

Introduction

Objectives

The overall audit objectives were to determine whether the Defense Civilian Pay System's (DCPS) general and application controls were adequately designed and effective to produce reliable data and whether the DCPS substantially complied with the Federal Financial Management Improvement Act of 1996 (Public Law 104-208) requirements and other applicable Federal and DoD information technology and information assurance policies. Appendix A discusses the audit scope and methodology, as well as prior audit coverage related to the audit.

This report supplements DoD Office of Inspector General Report No. D-2011-085, "Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness for the Period From October 1, 2010, Through April 30, 2011," July 15, 2011. The previous report concluded that controls were operating with sufficient effectiveness to provide reasonable, but not absolute assurance that DFAS officials achieved the following control objectives during the period from October 1, 2010 to April 30, 2011:

- An enterprise-wide security program was established, approved by management, monitored and tested, and maintained.
- Risk assessments were performed in accordance with applicable Federal and DoD requirements, and management reviews; and addressed risks as deemed appropriate by management.
- Management monitored compliance with policies and procedures and addressed instances of noncompliance.
- Management reviewed and authorized the hiring of and periodically evaluated employees with information assurance duties (staff), and out-processed terminated staff in accordance with applicable Federal and DoD requirements, and staff understood their documented duties.
- Management authorized, tested, approved, documented, and properly implemented changes to DCPS in accordance with management's defined requirements.
- Logical access to the DCPS application was granted to properly authorized individuals.
- DCPS computer processing was authorized and scheduled, and deviations from scheduled processing were identified and resolved.

- Personnel and payroll data transmitted to and from interfacing systems were transferred completely, accurately, and timely.

- Input data were authorized and were entered in DCPS completely and accurately.

- Personnel and payroll data processed and stored at DFAS and DCPS locations were authorized, complete, accurate, and timely processed, and the results of processing were recorded in audit trails.

- Output files were complete, accurate, and distributed in accordance with client specifications.

This report addresses whether DCPS complied with the Federal Financial Management Improvement Act (FFMIA) and whether physical security over DCPS data was adequate.

Background

The Defense Civilian Pay System (DCPS) processes pay for approximately 1.2 million employees, in accordance with existing regulatory, statutory, and financial information requirements related to civilian pay entitlements and applicable policies and procedures. DCPS pays all DoD civilian employees except local nationals, civilian mariners, and those supported by nonappropriated funds. In 1998, DCPS also began to pay personnel of the Executive Office of the President. As part of the 2001 President's Management Agenda e-Payroll Initiative, DCPS now processes payroll for the Departments of Energy, Veterans Affairs, and Health and Human Services; the Environmental Protection Agency; and the Broadcast Board of Governors. From a life-cycle perspective, DCPS is in the maintenance phase; its system changes are usually limited to legislative and functional requirements.

Other Matters of Interest

During the audit, we identified Performance Improvement Opportunities (PIOs) that do not require formal recommendations (Appendix B). In addition, Appendix C provides a status of all prior findings and recommendations associated with DCPS over the last five years.

Review of Internal Controls

DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," July 29, 2010, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. DFAS did not have the following internal controls for regulatory compliance and information: a self-assessment and remediation process for FFMIA compliance, and physical security over sensitive information. We will provide a copy of the report to the senior official for internal controls at the Defense Financial and Accounting Service.

Finding A. Assessing Federal Financial Management Improvement Act Compliance

DFAS officials did not comply with the FFMIA, as it relates to DCPS. Specifically, DFAS officials did not perform annual or complete self-assessments on DCPS to determine FFMIA compliance and did not develop a remediation plan to address requirements not met by DCPS. This occurred because DFAS officials were waiting on additional DoD guidance before pursuing FFMIA compliance further. Systems that do not comply with FFMIA requirements restrict the ability of organizations to consistently and accurately record the assets, liabilities, revenues, expenses, and the full costs of programs and activities of the Federal Government.

Federal Financial Systems Requirements

In 1996, Congress enacted the FFMIA (Public Law 104-208), which requires each agency to implement and maintain financial management systems that comply substantially with Federal financial management systems requirements, applicable Federal accounting standards, and the United States Government Standard General Ledger at the transaction level.

Office of Management and Budget Circular No. A-127, "Financial Management Systems," January 9, 2009, implemented the FFMIA. The Circular requires that agencies perform an annual review of their financial management systems to verify compliance with computer security and internal controls. If agencies do not use a system certified by the Financial Systems Integration Office, then the agencies may also be required to perform self-assessments of their core financial system. In addition, agencies must prepare a plan for their financial management systems that:

- describes the existing financial management system architecture, and any changes needed to implement a targeted architecture, and
- identifies projects necessary to achieve FFMIA substantial compliance within three years from the date of noncompliance.

DFAS's "Financial Management Systems Requirements Manual," (more commonly known as the Blue Book) is a comprehensive compilation of Federal and DoD financial management system requirements, as mandated by FFMIA. The requirements in the Blue Book document are applicable to accounting and finance systems operated and maintained by DFAS as well as "feeder" systems owned by the Military Services and DoD Components. The manual outlines specific requirements that DoD systems must satisfy to meet financial management requirements. The Blue Book identifies both the specific requirement, as well as the authoritative source of the requirement, and assists managers (who are responsible for financial management systems) in planning, designing, enhancing, modifying, and implementing financial management systems. Managers are ultimately responsible for being knowledgeable of and complying with the various authoritative sources of financial requirements (both legislative and regulatory).

Federal Financial Management Improvement Act Compliance for the Defense Civilian Pay System Needed Improvement

DFAS officials did not perform annual or complete self-assessments on DCPS to determine FFMIA compliance and did not develop a remediation plan to address requirements that DCPS did not meet.

Blue Book Requirements for DCPS Needed to be Reassessed

DFAS officials had not performed annual self-assessments to determine whether DCPS was compliant with current Blue Book requirements. DFAS officials performed the most recent self-assessment in 2009. DCPS is an entitlement system that provides pay and leave information to other financial systems to create reports, reconcile balances, deposit funds, provide information for core accounting systems to update their General Ledgers, and perform cost analysis. DCPS is also the payroll system for 5 of the 24 Agencies subject to the Chief Financial Officer's Act. DCPS also feeds an additional nine DoD financial statements required by the Office of Management and Budget. DFAS officials identified three volumes in the Blue Book that applied to DCPS in 2009:

DFAS Officials performed the most recent self-assessment in 2009.

- Volume 2 – Financial Reporting
- Volume 7 – Personnel Pay
- Volume 14 – Audit Trails and System Controls

However, DFAS updated the Blue Book three times since 2009. The January and May 2011 Blue Book updates added six new requirements (Requirement Identification Numbers 07.01.074, 07.06.086 through 07.06.089, and 07.08.006) to Volume 7 that DFAS officials should have assessed to determine applicability. In addition, although Volumes 2, 7, and 14 contained the majority of requirements applicable to DCPS, the January 2011 update included a new requirement (Requirement Identification Number 01.02.017) in Volume 1 that was also relevant:

> The Standard Financial Information Structure [SFIS] is required for "all target and legacy business feeder systems that will interface with a target system, as identified in the Enterprise Transition Plan that support financial transactions."

DCPS is a legacy business feeder system that will be part of DoD's business enterprise architecture. Accordingly, DCPS should be capable of feeding SFIS compliant data to agency systems that it supports (DoD and other federal agencies). Systems that do not comply with FFMIA requirements restrict the ability of organizations to consistently and accurately record the assets, liabilities, revenues, expenses, and the full costs of programs and activities of the Federal Government. A thorough review of current Blue Book requirements will enable DFAS officials to assess whether DCPS substantially complies with FFMIA.

A thorough review of current Blue Book requirements will enable DFAS officials to assess whether DCPS substantially complies with FFMIA.

DFAS Officials Needed to Update DCPS Self-Assessment

DFAS officials did not perform complete self-assessments. The 2009 self-assessment indicated that DCPS was compliant with 82 of 94 system requirements. However, for five system requirements (Requirement Identification No. 14.01.01, 14.02.52, 14.02.54, 14.02.55, and 14.04.09), DFAS officials did not determine whether DCPS was compliant, not compliant, or even whether the requirements were applicable to DCPS. For example, Requirement Identification No. 14.01.01 called for the system to generate an audit trail of transactions recorded as a document moves from the source through all document statuses. However, the self-assessment did not indicate whether DCPS did or did not comply with the requirement.

... DFAS officials did not determine whether DCPS was compliant, not compliant, or even whether the requirements were applicable to DCPS.

In addition, the self-assessment indicated that DCPS did not meet the requirement to use Public Key Infrastructure (PKI) certificates and biometrics for positive authentication (Requirement Identification No. 14.04.04). However, DFAS officials did not prepare a remediation plan that would address the non-compliance. The self-assessment stated that DCPS was a legacy system that did not use PKI and that DCPS employed user ID, password authentication, and regular monitoring, which are not substitutes for PKI. DoD's implementation of PKI uses two-factor authentication. Requiring two factors of authentication – "something you know," such as a Personal Identification Number and "something you have," such as a PKI-enabled Common Access Card – is called two-factor authentication. Two-factor authentication is a proven method for decreasing intrusions and other types of security breaches by ensuring that stolen user names and passwords are insufficient to gain access to networks.

Lastly, the self-assessment indicated that DCPS complied with the requirement to produce the reports and vouchers necessary to recognize payroll expenses, establish related receivables, and disburse all related payments to produce supporting detail registers or subsidiary ledgers (Requirement Identification No. 07.06.28). However, the self-assessment stated that although DCPS produced an automated file to accomplish disbursements and Treasury reporting, the file "[did] not meet all of the requirements that the accounting systems [had] developed." Consequently, DCPS may not have been fully

compliant with the requirement. DFAS officials should reassess whether DCPS fully meets this payroll system requirement.

FFMIA Compliance for DCPS Has Been a Long-Standing Issue

The DoD Inspector General (DoD OIG) issued three reports in prior years related to problems with completing DCPS self-assessments. These reports demonstrate long-standing difficulties that DFAS officials encountered while assessing DCPS compliance with FFMIA:

- DoD OIG Report No. D2010-074, "Information Assurance Controls for the Defense Civilian Pay System for FY 2009," August 2, 2010, stated that DCPS did not comply with FFMIA because DFAS did not test the mandatory requirements. During the audit, DFAS was still in the requirements analysis stage of the compliance process;
- DoD OIG Report No. D-2006-074, "Technical Report on the Defense Civilian Pay System General and Application Controls," April 12, 2006, stated that the DCPS Systems Management Office did not assess compliance since FY 2000 because they were waiting on direction from DFAS Headquarters; and
- DoD OIG Report No. D-2005-069, "Information System Security: Audit of the General and Application Controls of the Defense Civilian Pay System," May 13, 2005, concluded that the self-assessment had been completed using outdated guidance.

DFAS officials need to update the self-assessment using the current Blue Book requirements and make a determination on whether DCPS is compliant with each requirement that applies to the DCPS operating environment. Once the assessment is updated and complete, DFAS officials should prepare a remediation plan for instances of non-compliance.

Efforts to Determine Compliance

DFAS Information and Technology (I&T) personnel stated that they were waiting for Department-wide guidance to implement remediation plans through DFAS participation in DoD's Financial Improvement Audit Readiness initiative. At a minimum, however, DFAS officials needed to complete annual self-assessments and identify the projects needed to achieve FFMIA substantial compliance within three years.

Conclusion

DCPS is the payroll system for 5 of the 24 Agencies subject to the Chief Financial Officer's Act. DCPS also feeds an additional nine DoD financial statements required by the Office of Management and Budget. Systems that do not comply with FFMIA requirements restrict the ability of organizations to consistently and accurately record the assets, liabilities, revenues, expenses and the full costs of programs and activities of the Federal Government.

Recommendations, Management Comments and Our Response

We recommend that the Director, Defense Finance and Accounting Service:

A.1. Perform an annual review of the Defense Civilian Pay System, as required by Office of Management and Budget Circular No. A-127, to:

a. **Determine which Blue Book requirements apply to the Defense Civilian Pay System.**
b. **Determine which of the Blue Book requirements that apply to the Defense Civilian Pay System, cannot be performed.**

Defense Finance and Accounting Service Comments

The Director, I&T, responded for the Director, DFAS. He concurred and stated that the DCPS system/functional managers will conduct a self-assessment and identify applicable requirements. The Director, I&T indicated that the estimated completion date for the self-assessment review is August 31, 2012.

Our Response

The Director, I&T, comments on Recommendations A.1.a and A.1.b were responsive, and no additional comments are required.

A.2. Develop a remediation plan to address the requirements that Defense Civilian Pay System cannot perform.

Director, Information and Technology Comments

The Director, I&T, concurred and indicated that if the self-assessment finds DCPS not compliant, the system manager would identify required corrective actions and develop a remediation plan to bring DCPS into substantial compliance. The Director, I&T, indicated that the estimated completion date for developing a remediation plan is September 30, 2012.

Our Response

The Director, I&T, comments were responsive, and no additional comments are required.

Finding B. Physical Access Controls

DFAS Indianapolis personnel did not secure two of four Civilian Pay Operations locations at Indianapolis with cipher locks. This occurred because DFAS Indianapolis personnel had not completed required actions with the General Services Administration (GSA) to secure the locations. Without adequate controls over physical access, individuals could gain unauthorized access to computers and sensitive payroll data contained in online files and hardcopy printouts.

Information Assurance

DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003, implements the policies outlined in DoD Instruction 8500.1 by assigning responsibilities, and prescribing procedures for applying integrated, layered protection of the DoD information systems and networks. DoD Directive 8500.1 defines information assurance as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. The instruction requires DoD to assess information systems regularly for information assurance vulnerabilities and implement appropriate solutions to eliminate or otherwise mitigate identified vulnerabilities.

Physical Access Controls at Defense Finance and Accounting Service, Indianapolis, Needed Improvement

DFAS Indianapolis did not secure two of four Civilian Pay Operations locations with cipher locks. DoD Instruction 8500.2 requires every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release be controlled during working hours and guarded or locked during non-work hours. Although this deficiency was identified in two prior reports (D2009-001, "Information Assurance Controls for the Defense Civilian Pay System," dated October 7, 2008; and D2010-074, "Information Assurance Controls for the Defense Civilian Pay System for FY 2009," dated August 2, 2010), the office spaces at DFAS Indianapolis remained unsecured during our most recent audit. Securing all locations with cipher locks would reduce the risk that unauthorized individuals could:

> *...office spaces at DFAS Indianapolis remained unsecured during our most recent audit.*

- gain access to sensitive payroll data contained in hardcopy print outs and online files,
- obtain personally identifiable information for personal gain or introduce malicious code into DCPS, and
- obtain logical access to computer workstations used by Civilian Pay Operations employees to access DCPS.

Management Actions

We recognize that the payroll offices in Indianapolis were located in a Federal building and to install cipher locks required coordination between DFAS Indianapolis (the tenant) and GSA (the owner of the building with responsibility for building maintenance). DFAS Indianapolis officials provided funds to GSA for a new Access Control project that will establish lockable space in all areas and will consolidate Civilian Pay Operations to eliminate access concerns. DFAS Indianapolis expected to complete the project by the end of FY 2012. DFAS Indianapolis officials also stated that until the Access Control project is complete, Civilian Pay Operations has established interim internal controls such as visitor logs, mandatory visitor escorts, and signage stating "Authorized Personnel Only." Because we believe the management actions described above were sufficient, we made no recommendations associated with the access control issues identified in this report.

DFAS officials provided funds to GSA for a new Access Control project that will establish lockable space in all areas.

Appendix A. Scope and Methodology

We conducted this performance audit from January 2011 to May 2012, 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 assessed the design and operating effectiveness of the DCPS controls at three DFAS organizations. We developed audit procedures to test DCPS general and application controls using the Government Accountability Office Federal Information System Controls Audit Manual methodology and procedures prescribed in DoD Instruction 8500.2. In addition, we separated audit procedures into the following areas:

- **General Computer Controls.** These controls include the structure, policies, and procedures that apply to an entity's overall computer operations. General computer controls consist of entity-wide security management, access controls, configuration management, and segregation of duties.
- **Application Controls**. These controls directly relate to individual applications and are designed to ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. Application controls include programmed control techniques, such as automated edits, and manual follow-up of computer-generated reports, such as reviews of reports identifying rejected or unusual items.

We interviewed personnel at DFAS I&T in Indianapolis, Indiana, and DFAS payroll offices in Cleveland, Ohio, and Indianapolis, Indiana. We reviewed general and application controls in place only at DFAS organizations. We did not review application controls at any other payroll office or customer organization.

We did not review general controls performed by the Defense Information Systems Agency that provided direct or indirect administration and support of the operating environment used to host DCPS.

We did not test controls covering the originating systems that interface with DCPS. Controls at DCPS customer organizations were not included within the scope of this audit.

Use of Computer-Processed Data

We did not rely on computer-processed data to perform this audit.

Prior Coverage

During the last 5 years, the DoD IG has issued 6 reports discussing DCPS general and application controls. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports.

DoD IG Report No. D-2011-085 "Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness for the Period From October 1, 2010, Through April 30, 2011," July 15, 2011

DoD IG Report No. D-2010-074, "Information Assurance Controls for the Defense Civilian Pay System for FY 2009," August 2, 2010

DoD IG Report No. D-2010-071 "Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness for the Period From October 1, 2009, Through April 30, 2010," July 2, 2010

DoD IG Report No. D-2009-119, "Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness for the Period From October 1, 2008, Through June 30, 2009," September, 30, 2009

DoD IG Report No. D-2009-001, "Information Assurance Controls for the Defense Civilian Pay System," October 7, 2008

DoD IG Report No. D-2007-096, "Information Assurance Controls for the Defense Civilian Pay System," May 14, 2007

Appendix B. Performance Improvement Opportunities

We identified several PIOs during our review of DCPS. Implementation of these opportunities would allow DFAS to strengthen existing procedures and operational practices and gain additional process efficiencies. These observations are PIOs and we will not issue formal recommendations to DFAS.

Formal Termination and Transfer Account Deletion Procedures

DFAS Cleveland lacked formal termination and transfer procedures that established responsibilities and timeframes for terminating the access of Civilian Pay employees who leave or transfer from Civilian Pay. Although communication did occur between Human Resources and Civilian Pay, formalized procedures would help ensure that DFAS personnel timely and consistently remove access from all terminated and transferred employees.

DCPS Listing of Edit Checks

DFAS I&T DCPS system documentation contained a listing of application edits that included an outdated edit check no longer used by DCPS in the production environment. By maintaining a current listing of DCPS edit checks, DFAS I&T management would be better equipped to manage DCPS in an effective and efficient manner. Although there are no requirements, DFAS management should consider updating and maintaining DCPS system documentation to include a current listing of all DCPS edit checks.

592 Balancing Instructions

DFAS management had not updated DFAS 592 Balancing Instructions to include the supervisory review procedures, and the signatures and dates that were included on the 592 Reconciliations. Up-to-date 592 Balancing Instructions would help ensure that supervisors properly review, sign, and date the 592 Reconciliations. Although there are no requirements, DFAS management should consider updating and maintaining the 592 Balancing Instructions to include the supervisory review procedures and the signatures and dates that were included on the 592 Reconciliations.

Appendix C. Status of Prior Year Findings

The following table describes the status of all prior year findings that were open as of the initiation of the current year's audit.

Original Fiscal Year Finding Was Reported	Recommendation Number[1]	Finding Description	Open/ Closed	Management Response
2010	N/A	DFAS Standards and Compliance Division, which is responsible for monitoring control weaknesses and process issues identified in audits and self-assessments, did not track audit issues identified during the prior-year SAS 70 audit.	Closed	Management agreed with the exception in theory but provided clarity that DFAS tracks ONLY to recommendations that are included in a technical report for SAS 70 and the same is applied for all other audits internal and external. To remediate this exception, management will ensure going forward that we track to the draft SAS 70 report on issuance. Additionally, management believes this is an isolated incident and the control is working as intended.
2010	N/A	DFAS Human Resources could not provide an Out-Processing Checklist for one of two employees who separated from DFAS Cleveland during the examination period.	Closed	Management agreed with the exception, but in order to remediate this exception, management will work with DFAS Human Resources to ensure we have a defined process for ensuring all Out-Processing Checklists, both online and manual, are retained for separated employees.
2010	N/A	DFAS Saufley[2] did not sufficiently evidence the follow-up for 6 of 35 database or interface file data changes that were identified as unsupported by a valid change request during database and	Closed	Management agreed that additional follow-up is needed. The standard operating procedures for the Data Manipulation Language Online audit are being updated to include this additional level of review.

[1] Findings marked as 'Not Applicable' (N/A) were exclusively reported in prior year Statement on Auditing Standards No. 70 (SAS 70) and, as such, did not include a corresponding recommendation

[2] I&T organizations that administered DCPS were located at Saufley Field in Pensacola, Florida, prior to their move to Indianapolis, Indiana during the period October through December 2010. These organizations were commonly referenced within prior year audit reports as "DFAS Saufley."

Original Fiscal Year Finding Was Reported	Recommendation Number[1]	Finding Description	Open/ Closed	Management Response
		interface file change reviews performed for the months of October, November, and December 2009 and January 2010.		That update will include a reconciliation of the supervisor's comments to ensure every entry has been addressed and the action taken.
2010	N/A	DFAS Saufley did not ensure that all parties that are required to sign the DD 2875 user access form also annotated the date that they signed the form, as required. Specifically, for 1 of 36 sampled DCPS users, the information owner did not annotate the date that he/she signed the form.	Closed	Management agreed with the finding. DFAS Saufley created a new DD 2875 as soon as the employee returned to work.
2010	N/A	DFAS Saufley had implemented a privileged user access recertification process that does not require supervisors to evidence the specific user account(s) that they are recertifying. Additionally, DFAS Saufley had not implemented a process to validate that it periodically recertified each privileged user account.	Closed	Management agreed with the finding. Based on last year's audit report, DFAS took action to improve this review process by capturing and enforcing responses from management; however, the current process does include the formal review of user identifications and their associated access.
2010	N/A	DFAS Indianapolis used a manually maintained list of users to perform supervisory reviews of Civilian Pay employees with access to DCPS rather than system-generated user access listings.	Closed	Management agreed that this is not a system-generated list. This is a quarterly review and not a requirement or mandate. This is an additional control to the monthly DCPS audit reviews that the Indianapolis Payroll Office instituted, because of last year's SAS 70 report.

Original Fiscal Year Finding Was Reported	Recommendation Number[1]	Finding Description	Open/ Closed	Management Response
2010	N/A	DFAS Saufley has not consistently documented Memorandums of Agreement (MOAs) with customers to include the interface file type and frequency of files sent and received. Specifically, of 28 customer MOAs inspected: • 4 did not identify the frequency of files sent and received, and • 2 contained signatures obtained more than 3 years ago, thus rending the MOAs expired.	Open[3]	Management agreed with the exception in that MOAs are not consistently documented to identify the transmission type and the frequency of files sent and received. To remediate this exception, management is in the process of updating the MOAs.
2010	N/A	DFAS Saufley could not provide a consolidated listing of all of the data transmission completeness edit checks required by the service auditor in order to test the suitability of the design of the edit checks. As a result, the service auditor could not test the design or operating effectiveness of the data transmission completeness edit checks or the corresponding reviews performed by personnel at DFAS Saufley that rely on the outputs of the edit checks.	Closed	The DCPS Interface Specification is a 1,100+ page consolidated view of all user data formatting requirements for the 100+ types of DCPS interfaces and is systematically updated, as a DCPS configured item with every quarterly release. "Edits and validations" as defined by the audit team are at a level of detail beyond the existing DCPS Interface Specification. Based on estimates of the scope of the task and level of effort, management determined that defining all completeness checks and program edits/validations for 100+ interfaces for a very large system such as DCPS - with often multiple pre-processing and post-processing steps - has been cost prohibitive. This year's audit did, however, address testing of 20+ file completeness edits for 2 of the most critical DCPS interfaces – Source Data Automation and Personnel Data System - with no

[3] In our most recent report (DoD IG Report No. D-2011-085, *Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2010 through April 30, 2011)* we noted that this finding was still open. Of 27 MOAs selected for testing, one did not identify the transmission type of the files sent and/or received, three did not identify the frequency of files sent and received, and four contained signatures obtained more than three years ago.

Original Fiscal Year Finding Was Reported	Recommendation Number[1]	Finding Description	Open/ Closed	Management Response
				exceptions noted.
2010	N/A	DFAS Cleveland technicians did not record their initials and review dates for 1 of 24 Thrift Savings Plan (TSP) error reports inspected for testing.	Closed	Management agreed with the exception that annotations evidencing technician review for one TSP report were not present. In order to remediate this exception, management will ensure technicians annotate the TSP reports, as required. Additionally, management believes this is an isolated incident and the control is working as intended.
2010	N/A	DFAS Saufley did not sufficiently document the required destination for 44 of 45 sampled outgoing file transfers. Specifically, DFAS Saufley was unable to provide evidence of the intended destination (i.e., DCPS Action Request or e-mail) for 18 of the 45 outgoing file transfers selected for testing. Additionally, the destination within the documentation provided by the client did not match the destination within the file transfer table for 26 of the remaining outgoing file transfers selected for testing.	Closed	Management agreed that existing interface documentation does not consistently identify specific technical destinations (e.g., IP address, remote host name) as reflected in the DCPS table data provided for audit review. Direct traceability from a technical destination in a table entry to an originating customer request has not been a DCPS system requirement to date. While the DCPS project does monitor production jobs to ensure successful completion of outgoing file transfers, customers/end users of the data historically provide additional control measures to ensure receipt. Full remediation - to include changes in DCPS transfer table formats and direct customer contacts/reviews for the approx 6,800 physical file transfers in this interface population - would constitute a significant new workload and investment of DFAS resources.

Original Fiscal Year Finding Was Reported	Recommendation Number[1]	Finding Description	Open/ Closed	Management Response
2010	N/A	DFAS Cleveland did not reconcile the 592 checklist to the Report of Withholdings and Contributions for Health Benefits, Life Insurance, and Retirement Reports for 1 of 24 592 reconciliations. However, the unreconciled items did balance, and as a result, the 592 certification was correct. DFAS Cleveland did not reconcile the 592 checklist to the TSP Certification of Transfer for 6 of 24 592 reconciliations. However, the unreconciled items did balance, and as a result, the 592 certification was correct.	Closed Closed	Management agreed with the exception. However, the exception was found and corrected prior to the SAS 70 review by adding a formula to the checklist. No further problems were identified after that time, and the 592 certification was in balance. To correct the exception, DFAS Cleveland is developing individual spreadsheets and eliminating the monthly carry-forward process.
2010	Technical Report	DFAS Saufley did not clearly distinguish transfers from separations on the separations report.	Closed	This is a PIO and not a finding; therefore, no management responses were required
2010	Technical Report	DFAS Saufley did not have a process to establish criteria for determining the criticality of DCPS interfaces.	Closed	This is a PIO and not a finding; therefore, no management responses were required
2010	Technical Report	DFAS Cleveland's payroll technicians did not start with blank 592 reconciliation checklists each pay period.	Closed	This is a PIO and not a finding; therefore, no management responses were required
2010	Technical Report	DFAS Indianapolis did not require supervisor sign-off evidencing supervisor review of the TSP error report.	Closed	This is a PIO and not a finding; therefore, no management responses were required
2010	Technical Report	DFAS Indianapolis did not require annotations on the Duplicate Social Security Number report regarding issues requiring payroll technician follow-up action.	Closed	This is a PIO and not a finding; therefore, no management responses were required

Original Fiscal Year Finding Was Reported	Recommendation Number[1]	Finding Description	Open/ Closed	Management Response
2009	E.4	DFAS management did not implement standard operating procedures to include payroll input processing procedures. Specifically, DFAS Indianapolis did not document procedures for performing reviews and related follow-ups for the Personnel Interface Message Report and the New Hire Suspense Report. In addition, at DFAS Cleveland, the New Hire Suspense Report desktop procedures did not include review procedures and did not require supervisory review of the report.	Closed	The DFAS Director agreed with the recommendations and stated that DFAS would provide guidance and procedures for reviews and follow-ups for the Personnel Interface Message Report by October 1, 2010, and that it had implemented supervisory reviews of the New Hires report.
2009	A.1.a	The DFAS and Defense Information System Agency's certification and accreditation packages did not contain specific supporting documentation for each applicable DoD Instruction 8500.2 control. According to National Institute of Standards and Technology Special Publication 800-37, the security accreditation package should include the results of the security certification and provide the authorizing official with the essential information needed to make a credible, risk-based decision on whether to authorize operation of the information system.	Closed	The DFAS Director agreed with the recommendations and stated that DFAS included validation documentation to the DCPS certification and accreditation package on July 13, 2010.

Glossary

Application - software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. Examples include office automation, electronic mail, Web services, and major functional or mission software programs.

Availability - timely, reliable access to data and information services for authorized users.

Confidentiality - assurance that information is not disclosed to unauthorized entities or processes.

Data - representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities, to which meaning is or might be assigned.

Information Assurance (IA) - measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Integrity - quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Nonrepudiation - assurance that the sender of data receives proof of delivery and the recipient receives proof of the sender's identity, so neither can later deny having processed the data.

Sensitive Information - information for which the loss, misuse, unauthorized access to, or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled, but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Examples of sensitive information include, but are not limited to, information in DOD payroll, finance, logistics, and personnel management systems.

Defense Finance and Accounting Service Comments

DEFENSE FINANCE AND ACCOUNTING SERVICE
ARLINGTON
1851 SOUTH BELL STREET
ARLINGTON, VA 22240-5291

DFAS-ZT

MEMORANDUM FOR THE DOD INSPECTOR GENERAL

SUBJECT: Defense Finance and Accounting Service Needs to Strengthen Procedures to Comply with the Federal Financial Management Improvement Act (Project No. D2011-D000FB-0116.001)

Attached are management comments and action plans, with estimated completion dates for subject report. My point of contact is [redacted]

HINTON.JERRY[redacted]

Jerry S. Hinton
Director, Information and Technology

Attachment:
As stated

Defense Finance and Accounting Service Comments

Defense Finance and Accounting Service Needs to Strengthen Procedures to Comply with the Federal Financial Management Improvement Act (Project No. D2011-D000FB-0116.001)

We recommend that the Director, Defense Finance and Accounting Service:

A.1. Perform an annual review of the Defense Civilian Pay System, as required by Office of Management and Budget Circular No. A-127, to:

a. Determine which Blue Book requirements apply to the Defense Civilian Pay System.

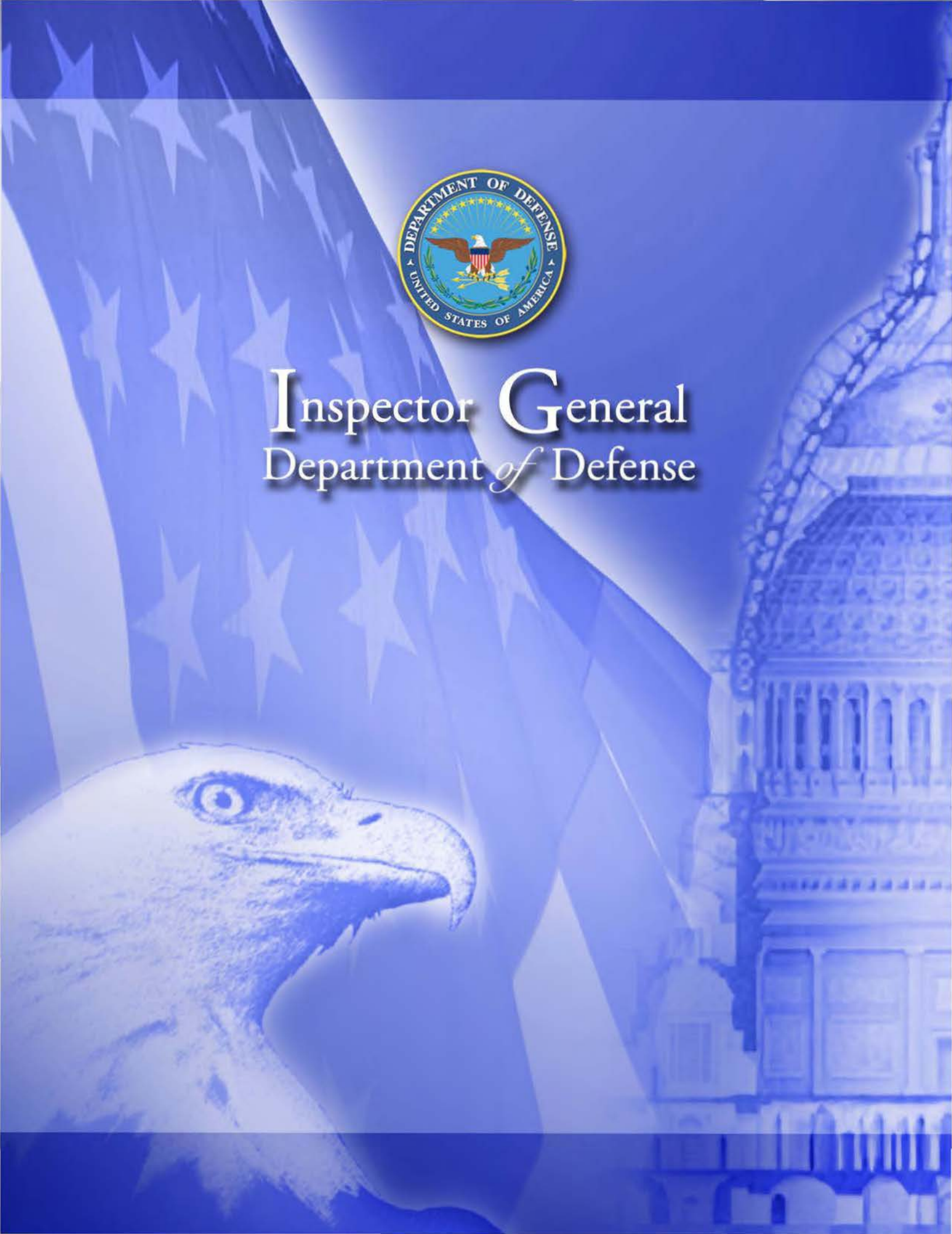
b. Determine which of the Blue Book requirements that apply to the Defense Civilian Pay System, cannot be performed.

Management Response: Concur

DCPS System/Functional Managers will conduct a Self Assessment Review and identify applicable requirements. **Estimated Completion Date:** August 31, 2012

A.2. Develop a remediation plan to address the requirements that Defense Civilian Pay System cannot perform.

Management Response: If DCPS is found not to be compliant, the System Manager will identify required corrective actions and develop a remediation plan to bring DCPS into substantial compliance. **Estimated Completion Date:** September 30, 2012.



Inspector General
Department of Defense