

# Inspector General

United States  
Department of Defense



Defense Civilian Pay System Controls  
Placed in Operation and Tests of  
Operating Effectiveness for the  
Period October 1, 2007,  
through March 31, 2008

### **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 (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

### **Suggestions for Future Audits**

To suggest ideas for or to request future audits, contact the Office of the Deputy Inspector General for Auditing at (703) 604-9142 (DSN 664-9142) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: Audit Suggestions)  
Department of Defense Inspector General  
400 Army Navy Drive (Room 801)  
Arlington, VA 22202-4704

DEPARTMENT OF DEFENSE

**hotline**

**To report fraud, waste, mismanagement, and abuse of authority.**

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900  
Phone: 800.424.9098 e-mail: [hotline@dodig.mil](mailto:hotline@dodig.mil) [www.dodig.mil/hotline](http://www.dodig.mil/hotline)



INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
400 ARMY NAVY DRIVE  
ARLINGTON, VIRGINIA 22202-4704

September 30, 2008

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE  
(COMPTROLLER)/CHIEF FINANCIAL OFFICER  
ASSISTANT SECRETARY OF DEFENSE (NETWORKS  
AND INFORMATION INTEGRATION)/DOD CHIEF  
INFORMATION OFFICER  
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING  
SERVICE  
DIRECTOR, DEFENSE INFORMATION SYSTEMS  
AGENCY

SUBJECT: Report on Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2007, through March 31, 2008 (Report No. D-2008-139)

We are providing this report for your information and use. No written response to this report is required. Therefore, we are publishing this report in final form.

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Patricia Remington at (703) 601-5815 (DSN 329-5815) or Mrs. Donna A. Roberts at (703) 601-5859 (DSN 329-5859). The team members are listed inside the back cover.

*Patricia A. Marsh*  
Patricia A. Marsh, CPA  
Assistant Inspector General  
Defense Financial Auditing Service



# Table of Contents

---

<b>Foreword</b>	i
<b>Section I</b>	
Independent Service Auditor's Report	1
<b>Section II</b>	
Description of the Defense Civilian Pay System Operations and Controls Provided by the Defense Finance and Accounting Service and the Defense Information Systems Agency	13
<b>Section III</b>	
Control Objectives, Control Activities, and Tests of Operating Effectiveness	25
<b>Section IV</b>	
Supplemental Information Provided by the Defense Finance and Accounting Service and the Defense Information Systems Agency	113
<b>Acronyms and Abbreviations</b>	117



## **Foreword**

This report is intended for the use of the Defense Finance and Accounting Service (DFAS) and the Defense Information Systems Agency (DISA) management, its user organizations, and the independent auditors of its user organizations. DoD personnel who manage and use the Defense Civilian Personnel System (DCPS) will also find this report of interest as it contains information about DCPS general and application controls.

The DoD Office of Inspector General (OIG) is implementing a long-range strategy to conduct audits of DoD financial statements. The Chief Financial Officers Act of 1990 (Public Law 101-576), as amended, mandates that agencies prepare and conduct audits of financial statements, which is key to achieve the goals of the Chief Financial Officers Act.

The DCPS is a pay processing system used to pay DoD civilian employees, as well as employees at several other Federal entities, including the Departments of Energy, Health and Human Services, and the Executive Office of the President. As of March 31, 2008, DCPS processes pay for approximately 834,000 employees.

This audit assessed controls over the DCPS processes at DFAS and DISA. This report provides an opinion on the fairness of presentation, the adequacy of design, and the operating effectiveness of key controls that are relevant to audits of user organization financial statements. As a result, this audit precludes the need for multiple audits of DCPS performed by user organizations to plan or conduct financial statement and performance audits. Effective internal control is critical to achieve reliable information for all management reporting and decision making.





---

**Section I: Independent Service Auditor's Report**

---





INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
400 ARMY NAVY DRIVE  
ARLINGTON, VIRGINIA 22202-4704

September 30, 2008

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (COMPTROLLER)/  
CHIEF FINANCIAL OFFICER  
ASSISTANT SECRETARY OF DEFENSE (NETWORKS  
AND INFORMATION INTEGRATION)/DOD CHIEF  
INFORMATION OFFICER  
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING  
SERVICE  
DIRECTOR, DEFENSE INFORMATION SYSTEMS  
AGENCY

SUBJECT: Report on Defense Civilian Pay System Controls Placed in Operation and  
Tests of Operating Effectiveness for the Period October 1, 2007, through  
March 31, 2008

We examined the accompanying description of the general computer and application controls related to the Defense Civilian Pay System (DCPS) (Sections II and III). The Defense Finance and Accounting Service-Headquarters (DFAS-HQ) provides management control and coordination within DoD and has overall responsibility for the DCPS. DCPS is maintained and supported by the DFAS technical support elements and the Defense Information Systems Agency (DISA). Therefore, the DCPS general computer and application controls are managed by both DISA and DFAS. Our audit included procedures to obtain reasonable assurance that (1) the accompanying description presents fairly, in all material respects, the aspects of the controls at DFAS and DISA that may be relevant to a DCPS user organization's internal controls as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and user organizations applied those aspects of internal controls contemplated in the design of the controls at DFAS and DISA; and (3) such controls had been placed in operation as of March 31, 2008.

The control objectives were specified by the DoD Office of the Inspector General (OIG). We performed our audit in accordance with American Institute of Certified Public Accountants standards and applicable financial audit standards contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and included those procedures we considered necessary to obtain a reasonable basis for rendering our opinion.

DCPS's general computer control environment includes certain controls that are pervasive across the DISA Defense Enterprise Computing Center (DECC) Mechanicsburg (DECC-MECH) data center that houses and supports DCPS.

These types of pervasive controls include:

- overall security planning (for example, DECC risk assessments, site security plans, security management structure);
- general employee processes (for example, background investigations and position and job descriptions);
- group authentication;<sup>1</sup> and
- physical security:
  - visitor access;
  - network administration (for example, firewalls, network scans, remote access, network monitoring, use of mobile code);
  - incident response;
  - environmental controls; and
  - hardware maintenance.

We did not examine these pervasive controls at the DISA DECC-MECH data center because these controls were evaluated as part of the DISA Statements of Auditing Standard No. 70 (SAS 70) and excluded from the scope of this audit at the direction of the DoD OIG.

The accompanying description includes those application control objectives and related controls resident at the Charleston, South Carolina; Pensacola, Florida; Indianapolis, Indiana; Cleveland, Ohio; and Denver, Colorado Payroll Offices. However, due to the payroll office consolidation as a result of the Base Realignment and Closure (BRAC), the Charleston and Denver Payroll Offices permanently closed during this audit. In addition, the Pensacola Payroll Office permanently closed on May 31, 2008. The remaining payroll offices in Indianapolis, Indiana, and Cleveland, Ohio, performed the control activities. Therefore, we did not inspect controls specific to the closed locations as part of this audit.

DCPS processes approximately 81 interface files from DoD and external systems. Examples of systems that provide interface files<sup>2</sup> to DCPS include the Defense Civilian Personnel Data System, Federal Reserve, Thrift Savings Plan, and the Department of Treasury. The accompanying description does not include control objectives and general and application controls related to the systems that interface with DCPS. In addition, our audit did not extend to the controls at the National Security Agency (NSA). Furthermore,

---

<sup>1</sup> The act of verifying the identity of a user and the user's eligibility to access computerized information. Designed to protect a system against fraudulent activity.

<sup>2</sup> A connection between two devices, applications, or networks or a boundary across which two systems communicate.

because of the sensitive nature of the pay information for personnel who work for the Executive Office of the President (EOP), our audit did not extend to the controls over EOP payee transactions.

We conducted our audit for the purpose of forming an opinion of the description of the DCPS general and application controls at DFAS and DISA (Sections II and III). We have included information about business continuity plans and procedures at DFAS and DISA, as provided by DFAS and DISA respectively in Section IV. Section IV only provides additional information to user organizations and is not a part of the description of controls at DFAS and DISA. The information in Section IV has not been subjected to the procedures applied in the audit of the controls at DFAS and DISA. Accordingly, we do not express an opinion on the description of DFAS and DISA business continuity plans and procedures.

We identified the following control design deficiencies related to the controls described in Section III, Control Objectives, Control Activities, and Tests of Operating Effectiveness.

### **Lack of Approved Policies**

We noted that no policy exists that requires Civilian Pay Processing personnel to generate and review a complete, accurate listing of management summary reports to confirm that payroll is processed timely and accurately. In addition, we noted there was no policy for retaining 592 documentation; specifically, the 592 Report Checklist and the 592 Report of Withholdings. We also noted that there was no policy at DFAS Indianapolis for the physical security of the pay processing areas.

As a result, the design of the controls does not provide reasonable assurance that the following control objectives will be achieved.

*“Controls prevent unauthorized system access to DCPS data.”*

*“Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA General Computer Control locations are valid, accurate, authorized, complete, timely, support financial reporting requirements and provide sufficient audit trails.”*

As discussed in Sections II and III, DFAS and DISA have developed policies and procedures to ensure that personnel and payroll data processed and stored at DFAS and DISA are valid, accurate, authorized, complete, timely, support financial reporting requirements, and provide sufficient audit trails. However, these policies have not been consistently updated or followed by DFAS. As a result, the design of DFAS controls does not provide reasonable assurance that the control objectives, “Controls prevent unauthorized system access to DCPS data”; and “Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA General Computer Control locations are valid, accurate, authorized, complete, timely, support financial reporting requirements and provide sufficient audit trails,” will be achieved.

In our opinion, Sections II and III present fairly, in all material respects, the relevant aspects of DFAS and DISA controls that had been placed in operation as of March 31, 2008. Also, in our opinion, except for the design deficiency referred to in the preceding paragraph, the controls are suitably designed to provide reasonable, but not absolute, assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied those aspects of internal control contemplated in the design of the DFAS and DISA controls.

In addition to the procedures that we considered necessary to render our opinion, as expressed in the previous paragraph, we tested specified controls, listed in Section III, to determine whether they are effectively meeting the related control objectives described in Section III during the period of October 1, 2007, through March 31, 2008. We documented the specific control objectives and controls. We also documented the nature, timing, extent, and results of the tests in Section III. We provided this information to DCPS user organizations and to their auditors to be taken into consideration, along with information about the user organizations' internal control environments, when making assessments of control risks for such user organizations.

We identified the following operating deficiencies related to the controls described in Section III, Control Objectives, Control Activities, and Tests of Operating Effectiveness.

#### **DCPS User Access**

DFAS requires every DCPS user to complete a System Access Authorization Request (SAAR) form. The SAAR form documents user access and must be signed by a supervisor indicating that such access has been approved. Upon selecting a sample of 90 forms for DCPS non-payroll office users, we determined that:

- 15 forms could not be located,
- 11 forms had a user type that did not match the user type in the list of DCPS Users by Database,
- 6 forms had authorization types that did not match the authorization type in the list of DCPS Users by Database,
- 16 forms were missing the DCPS Security Awareness Computer-Based Training completion date,
- 1 form was missing the user's signature,
- 2 forms were missing the supervisor's signature,
- 10 forms were missing the date of the supervisor's signature,
- 23 forms were missing the security manager's signature,

- 27 forms were missing the date of the security manager's signature, and
- 13 users completed the incorrect form.

Upon selecting a sample of 90 forms for DCPS payroll office users, we identified that:

- 10 forms could not be located,
- 29 users completed the incorrect form,
- 31 forms had a user type that did not match the user type in the list of DCPS Users by Database,
- 11 forms were missing the DCPS Security Awareness Computer-Based Training completion date,
- 1 form was missing a user's signature,
- 6 forms were missing the date of the supervisor's signature,
- 10 forms were missing the security manager's signature, and
- 17 forms were missing the date of the security manager's signature.

Upon examining forms for the entire population of 66 users with the ability to disburse payroll, we identified 1 form that did not contain justification for access to disburse payroll.

As a result, the following control objectives may not have been achieved during the period of October 1, 2007, through March 31, 2008.

*“Controls prevent unauthorized system access to DCPS data.”*

*“Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA General Computer Control locations are valid, accurate, authorized, complete, timely, support financial reporting requirements and provide sufficient audit trails.”*

### **Monitoring DCPS Error Reports**

The Personnel Interface Invalid Report (PIIR) is a key control for monitoring and resolving DCPS interface processing errors. This report contains rejections, suspensions, or deletions of data to document changes in existing data in DCPS and data input through interface files.

We examined a sample of 45 PIIRs generated during the audit period at each payroll office to confirm whether the reports were consistently annotated to indicate that processing exceptions were resolved.

At the DFAS Indianapolis Payroll Office, 12 of the 45 PIIRs selected from five databases could not be located. Of the remaining 33 reports inspected, we identified that:

- 2 reports were missing the date of when the report was annotated by the technician and
- 3 reports were not correctly annotated with codes outlined in the Standard Operating Procedure (SOP).

At the DFAS Cleveland Payroll Office, 16 of the 45 PIIRs selected from five databases could not be located. Of the remaining 29 reports inspected, we identified that:

- 1 report was missing a technician's signature and
- 1 report was missing the date of when the report was reviewed by the technician.

As a result, the following control objective may not have been achieved during the period of October 1, 2007, through March 31, 2008.

*“Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA locations are valid, accurate, authorized, complete, timely, support financial reporting requirements and provide sufficient audit trails.”*

### **Visitor Access**

At the DFAS Cleveland Payroll Office, we inspected a sample of 21 visitor logs. Of the 21 visitor logs inspected, we observed that:

- 4 logs were missing the visitor organization,
- 4 logs were missing the authorized sponsor,
- 3 logs were missing the reason for visit,
- 4 logs were missing the floor visited, and
- 4 logs were missing the visitor badge turn-in date.

At the DFAS Indianapolis Payroll Office, visitors with a valid Common Access Card, law enforcement badge, or military identification can enter the DFAS building and are not required to sign in and out with security; therefore, access is not limited to authorized payroll office personnel. We observed that the terminals that process payroll are located in a physically secure building. However, terminal rooms are not locked, and data entry terminals can be connected to the system 24 hours a day, 7 days a week, except during system downtime. The terminal rooms are located in shared spaces with other agencies and non-payroll office personnel have access to sensitive payroll information. We also observed that the cabinets where payroll information is stored are not secured. In addition, we observed that visitors to the DFAS Indianapolis Payroll



Office must sign in and out with authorized security personnel; however, once the visitor is inside the building there is no requirement to display the visitor badge.

As a result, the following control objective may not have been achieved during the period of October 1, 2007, through March 31, 2008.

*“Controls prevent unauthorized physical access to DCPS data.”*

### **Management Summary Reports**

The Indianapolis and Cleveland Payroll Offices lacked a policy that requires a complete listing of summary reports to confirm that personnel and payroll data are processed, valid, accurate, and authorized.

As a result, the following control objective may not have been achieved during the period of October 1, 2007, through March 31, 2008.

*“Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA General Computer Controls locations are valid, accurate, authorized, complete, timely, support financial reporting requirements and provide sufficient audit trails.”*

### **Personnel/Payroll Reconciliation Reports**

At the DFAS Indianapolis Payroll Office, we inspected 45 Personnel/Payroll Reconciliation Reports. The Personnel/Payroll Reconciliation Reports document the reconciliation between the personnel systems of the payroll customers and DCPS to capture changes in personnel information. Of the 45 Personnel/Payroll Reconciliation Reports inspected, 1 report could not be located. In addition, eight reports did not include notification sent to user agencies with the necessary changes.

At the DFAS Cleveland Payroll Office, we found that the DFAS Cleveland Payroll Office did not receive any Personnel/Payroll Reconciliation Reports for two quarters of the audit period.

As a result, the following control objective may not have been achieved during the period of October 1, 2007, through March 31, 2008.

*“Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA General Computer Controls locations are valid, accurate, authorized, complete, timely, support financial reporting requirements and provide sufficient audit trails.”*

### **592 Reconciliation Reports**

The 592 Reconciliation process is performed at the end of every pay period by civilian pay technicians to confirm that all payroll balancing spreadsheets have been received and all

discrepancies have been identified and/or corrected in order to release payroll files to the disbursing office.

At the DFAS Indianapolis Payroll Office, we inspected 45 592 Reconciliation reports. Of the 45 592 Reconciliation reports, 8 reports did not have documentation of a final disbursement authorization.

We noted that 1 of 45 selected 592 Reconciliations did not balance, and a supplemental 592 Reconciliation was not prepared. We noted that for 1 of 45 selected 592 Reconciliations, the Report of Withholdings was not signed.

As a result, the following control objectives may not have been achieved during the period of October 1, 2007, through March 31, 2008.

*“Controls provide reasonable assurance that DCPS authorized users are restricted to access only areas needed to complete their assigned responsibilities and controls maintain segregation of duties.”*

*“Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA General Computer Controls locations are valid, accurate, authorized, complete, timely, support financial reporting requirements and provide sufficient audit trails.”*

### **DCPS Change Management**

All configuration changes made to the DCPS application are required to comply with Department of Defense Instruction 8500.2, “Information Assurance Implementation,” standards for software development change controls. However, the configuration management process at DISA does not provide an audit trail to confirm that changes are tested in a test environment before being implemented into the production environment.

As a result, the following control objectives may not have been achieved during the period of October 1, 2007, through March 31, 2008.

*“DISA or DFAS initiated application, software, or hardware modifications are authorized, and the documentation is maintained.”*

*“Changes to the DoD information system are assessed for Information Assurance (IA) and accreditation impact prior to implementation.”*

## **DCPS Access Audits**

Monitoring access to DCPS is required to comply with DoD Instruction 8500.2 standards for audit trails, monitoring, analysis, and reporting. However, payroll office personnel did not perform the monthly access audits.<sup>3</sup>

As a result, the following control objective may not have been achieved during the period of October 1, 2007, through March 31, 2008.

*“Audit trails are maintained.”*

## **DCPS Operator Logs**

Access to DCPS is required to comply with DoD Instruction 8500.2 standards for group identification and authentication. However, the DFAS operations group uses a group authenticator to execute batch jobs. To mitigate risk, DFAS uses a daily operator log to record the actions of the operators. However, DFAS could not provide operator logs for 3 of 18 sampled dates.

As a result, the following control objectives may not have been achieved during the period of October 1, 2007, through March 31, 2008,

*“Group authenticators for application or network access may be used only in conjunction with an individual authenticator.”*

*“Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA General Computer Controls locations are valid, accurate, authorized, complete, timely, support financial reporting requirements and provide sufficient audit trails.”*

In our opinion, except for the deficiencies in operating effectiveness noted in the preceding paragraphs, the controls that we tested, as described in Sections II and III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Sections II and III were achieved during the period of October 1, 2007, through March 31, 2008.

The relative effectiveness and significance of specific controls at DFAS and DISA, and their effect on assessments of control risk at user organizations, are dependent on their interaction with the internal control environment and other factors present at individual user organizations. We have not performed procedures to evaluate the effectiveness of internal controls placed in operation at individual user organizations.


The description of the controls at DFAS and DISA is as of March 31, 2008, and information about tests of their operating effectiveness covers the period of October 1,

---

<sup>3</sup> DCPS conducts three types of internal audits at the payroll offices: user access, segregation of duties, and supervisory codes.

2007, through March 31, 2008. Drawing any conclusions or making any projection of such information on the future based on our findings is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiveness of specific controls at DFAS and DISA is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected.

This report is intended solely for use by DCPS management, its user organizations, and the independent auditors of such user organizations.

  
Patricia A. Marsh, CPA  
Assistant Inspector General  
Defense Financial Auditing Service

---

**Section II: Description of the Defense Civilian Pay System  
Operations and Controls Provided by the Defense Finance and  
Accounting Service and the Defense Information Systems  
Agency**

---



## **II. Description of the Defense Civilian Pay System Operations and Controls Provided by the Defense Finance and Accounting Service and the Defense Information Systems Agency**

### **A. Overview of DCPS**

#### **Purpose of DCPS**

In 1991, DoD selected DCPS as its standard payroll system. DCPS is used by all DoD activities paying civilian employees, except Local Nationals and those funded by Non-appropriated Funds and Civilian Mariners. Before becoming the DoD-wide civilian pay system, DCPS was the Navy civilian pay system, which had been in operation since 1988. DFAS began paying the Executive Office of the President (EOP) in 1998. The 2001 President's Management Agenda e-Payroll initiative established federal payroll providers to service the entire executive branch of the Federal Government; DFAS was selected as one of those providers. DFAS began processing payroll for the Department of Energy (DoE) in 2003, the Department of Health and Human Services (HHS) in 2005, the Environmental Protection Agency (EPA) and, Department of Veterans Affairs (VA) in 2006, and the Broadcast Board of Governors (BBG) in 2007. As of June 30, 2008, DCPS currently processes pay for approximately 834,000 employees.

The DCPS program mission is to process payroll for DoD and non-DoD civilian employees in accordance with existing regulatory, statutory, and financial information requirements relating to civilian pay entitlements and applicable policies and procedures. The DoD civilian pay program must satisfy the complex and extensive functional, technical, and interface requirements associated with the DoD and non-DoD civilian pay function. The functional areas include: employee data maintenance, time and attendance, leave, pay processing, deductions, retirement processing, debt collection, special actions, disbursing and collection, reports processing and reconciliation, and record maintenance and retention. DCPS provides standard interface support to various accounting, financial management, and personnel systems. From a life cycle perspective, DCPS is in the maintenance phase, with system changes mainly resulting from legislative and functional requirements.

DFAS participated in a BRAC transformation that impacted the DCPS Payroll Offices. The BRAC consolidated and relocated the three servicing payroll offices located in Pensacola, Florida, Charleston, South Carolina and Denver, Colorado into two payroll offices located in Cleveland, Ohio, and Indianapolis, Indiana. The move and consolidation were completed in March, 2008. Approximately 300 payroll processing personnel at the two DFAS Payroll Offices use DCPS. DCPS is also used at NSA<sup>4</sup>. Additional users include Customer Service Representatives (CSRs), Timekeepers, and

---

<sup>4</sup>The NSA payroll office is not included in the scope of this "Description of DCPS Operations and Controls Provided by DFAS and DISA."

Certifiers at customer activities and sites. The Cleveland Payroll Office processes payroll for the Navy, DoE, and HHS. The Indianapolis Payroll Office processes payroll for all other unclassified DFAS payroll customers. Migration of VA pay account processing is scheduled for completion September, 2009.

### **DCPS Support Functions**

The DFAS Standards and Compliance Division (under the cognizance of the DFAS Director) provides high-level management control and coordination within DoD and for DCPS external customers. The Civilian Pay Systems Management Directorate (under the cognizance of the DFAS Chief Information Officer) have overall daily responsibility for application, operation, interpretation and implementation of DCPS. In addition, those offices are responsible for coordinating with external users and new customers. Civilian Pay Systems Management Directorate is responsible for requirements management, functional analysis, information assurance, and user documentation processes.

The Technology Services Engineering Organization Pensacola (TSOPE) provides DCPS software engineering, production support, and customer service. Within TSOPE, several groups provide DCPS support. The Software Engineering Division provides technical design, programming, unit testing, and system documentation. The Software Test and Evaluation Division performs integration testing and evaluation processes. The Project Support Division provides system software, telecommunication, computer resource tools, and database support. DCPS Software Quality Assurance monitors the software engineering process and provides recommendations for improvement. The Systems Support Division provides configuration management, release management, implementation status, and customer support. DCPS is maintained and executed on a DISA mainframe platform at DISA DECC-MECH, Pennsylvania.

### **DCPS Systems Architecture**

DCPS has a two-tiered architecture comprised of the following:

- Mainframe hardware and software components - used as a repository for collecting and accumulating data, and providing centralized, biweekly processing of civilian pay and its attendant functions (for example., electronic funds transfer, generation of leave and earnings statements); and
- Remote user/print spooler hardware and software - used to collect and/or pre-process data at customer sites, provide connectivity to DCPS mainframe components, and support printing of mainframe-generated outputs (for example, reports, timesheets) at customer locations. The components are largely customer-owned and operated, and include local area networks (LANs), personal computers, and a diverse assortment of printers and software that operates and connects the networks, computers, and printers. DFAS maintains a limited number of mid-tier (minicomputer) systems at selected DFAS sites to handle specialized printing requirements (for example, paychecks). Other offloaded print services, such as bulk printing for DCPS Payroll Offices and printing of Leave and Earnings Statements, are performed on Personal Computer/workstation hardware



maintained by the Document Automation & Production Service (DAPS) at sites located in various U.S. and overseas geographical regions.

The two tiers of the DCPS architecture are connected through DoD-maintained networks comprised of Internet Protocol (IP)-based (for example, Non-Classified Internet Protocol Router Network (NIPRNET)) and Systems Network Architecture (SNA)-based (leased line) services. Those networks connect DCPS to a wide variety of external, non-DCPS sites (mainframes, mid-tiers, and PCs) that supply or exchange data with DCPS, mainly through electronic file transfers, on a regular basis. Examples of external interface sites include the Defense Civilian Personnel Data System, Thrift Savings Plan (TSP), Department of the Treasury, and non-DoD users such as DoE, EPA, EOP, HHS, BBG, and VA.

The main technical components of DCPS include the following attributes.

- DCPS is housed in a separate logical domain on an IBM z9 mainframe computer located at DISA DECC-MECH,
- The IBM mainframe operating system software is z/OS release 1.9,
- DCPS is written in Common Business Oriented Language II,
- First point of entry security protection mechanisms are provided by Access Control Facility 2 (ACF2),
- DISA DECC-MECH provides four web servers that service all applications that support DCPS. Those servers accept the users' secure web requests by supplying a menu screen with options for each application to the DCPS LOGON SCREEN, where individuals enter their ACF2 login user identification (ID) and passwords,
- Third-party software packages are used for DCPS process scheduling and monitoring, tax calculations, and mailing address verification.

The payroll offices and associated CSRs have access to DCPS through dedicated leased lines, various DoD networks, and through Multi-Host Internet Access Portal, formally known as Mainframe Internet Access Portal (MIAP). MIAP enables secure transaction processing across the NIPRNET. Attachmate's Reflection for the Web product was used to establish a secure infrastructure utilizing Virtual Private Network (VPN) encryption through the DoD DMZs. DCPS users interact directly with the DCPS application through "3270" emulation using Personal Computer/Advanced Technology keyboard mapping terminals or terminal simulation programs for communication with DCPS. This permits application-defined formatted screens to be displayed with protected static text and unprotected fields for data entry.

In addition, the operating site is networked with TSOPE to support DCPS software releases and production support.

- Terminals. Some DFAS DCPS users will use Internet Protocol Telenet RUMBA 3270 emulation package across dedicated lines with extended attributes and PC/AT keyboard mapping, terminals, or terminal simulation programs (PCs) for communication with the application. This permits application-defined formatted screens to be displayed with protected static text and unprotected fields for data entry. Once the screen is formatted for a type of transaction, only the data entered is transmitted between the terminal and the mainframe.
- Printers. Printers provide printing support for majority of Payroll Office and Systems printing requirements. All printing goes through VPN IP Protocol.
- MIAP. DISA DECC-MECH provides access to DCPS through the MIAP. The DCPS user community may access the system using DISA's inherited MIAP solution across the Internet using an authorized Internet browser. PKI Authentication is maintained at the MIAP server, and user ID/ password authentication is still maintained at the DCPS application logon.

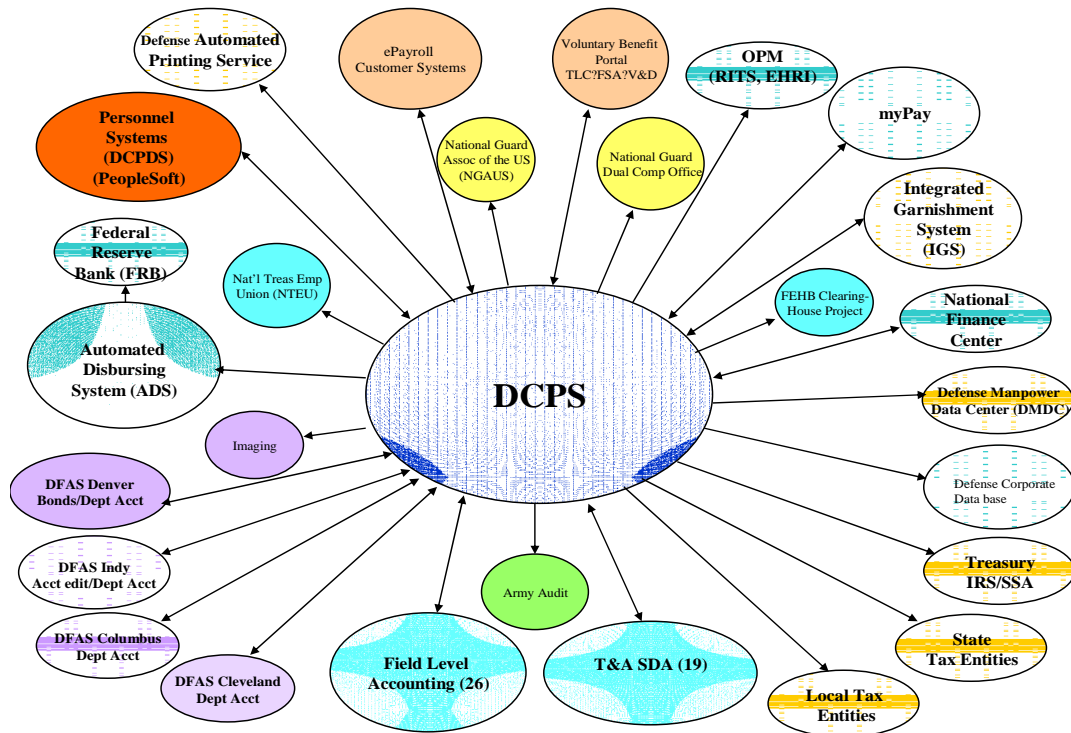
The payroll offices are structured in accordance with DFAS standard staffing policy and conduct business using standard operating and support procedures. They operate on a 24-hour basis to provide payroll service to customers located in various time zones and are responsible for the full range of pay processing functions and services. As circumstances dictate, the three payroll offices serve as operational back-up sites for each other when contingency procedures are executed by DFAS.

DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003, (DoD I 8500.2) identifies specific control requirements DoD systems should achieve based on their designated Mission Assurance Category (MAC). The DCPS application Authority to Operate, dated July 29, 2005, is on file with the DFAS Chief Information Officer, and reaccreditation package is awaiting approval. According to the current DCPS System Security Authorization Agreement (SSAA), as of June 30, 2005, the MAC level for the DCPS application is "MAC III" and its supporting enclave at DISA DECC-MECH is "MAC II".

### **DCPS Data Flow**

The figure below depicts the flow of data to and from DCPS. DCPS customers and technicians input data, including master employee and time and attendance logs. DCPS outputs data to multiple systems and entities, including financial reporting entities, the automated disbursing system and data storage.

# DCPS Interfaces



## Overview of System Interfaces

DCPS is a combination of on-line and batch programs that support the requirements of a bi-weekly payroll process for civilian employees in the Federal Government based on data feeds from numerous personnel, accounting, and time and attendance systems. Transactions to update employee data, adjust leave balances and payments, and report time and attendance may be input daily to spread the on-line workload and to obtain labor data. However, the focal point of the system is the bi-weekly process. Non bi-weekly process functions occur monthly, quarterly, annually, or as required, and are in support of or a result of, multiple bi-weekly pay cycles. DCPS supports a standard personnel interface, decentralized time and attendance reporting, and the CSR structure.

DCPS accepts input from three primary areas: CSR, timekeepers, and personnel offices. DCPS receives or creates approximately 81 interface files that, among other functions:

- update personnel information,
- upload time and attendance data,
- download information for checks to be printed,
- report accounting information to the Department of the Treasury,

- reconcile enrollment information with health care providers, and
- download general accounting information to DoD agencies.

Automatic electronic files transfer directly to and from the host mainframe computer is preferred for input and output file interfaces. Output files are automatically transmitted to sites and activities using common file transfer protocols, through communication lines of files written to magnetic tape at the host (per data in File Transfer Tables). Interface partners must provide File Transfer Table data to the TSOPE for table updates. For files not automatically transferred, the activity receiving DCPS data is responsible for accessing the host computer to retrieve (“pull”) the output file(s) from the host. In addition, the activity creating payroll data is responsible for developing and sending a DCPS input file by secure means to the processing center supporting the payroll office. The payroll activities and the submitting activities establish mutually agreeable schedules to ensure timely receipt of data necessary to support DCPS payroll processing. TSOPE is responsible for executing and monitoring interface processing, as well as resolving interface processing errors or problems.

## **B. Control Environment**

### **DCPS Management Oversight**

The DFAS Information and Technology Directorate is responsible for reviewing and approving DCPS security policy and its certification and accreditation plan, and granting DCPS authority to operate. TSOPE provides not only DCPS software engineering support, but also production support and customer service. DCPS is maintained and executed on a DISA mainframe platform at DISA DECC-MECH, Pennsylvania. DISA DECC-MECH is part of the Center for Computing Services within the Global Information Grid Combat Support Directorate, which is a Strategic Business Unit within DISA. DFAS and DISA have documented DCPS support services provided by DISA in a service-level agreement that is reviewed by both agencies on an annual basis. DFAS and DISA have documented policies and procedures describing their respective roles and responsibilities in supporting payroll functions. DISA and DFAS are Defense agencies that report to the Office of the Secretary of Defense.

### **Personnel Policies and Procedures**

#### *DFAS Payroll Offices and TSOPE*

Payroll office employees and contractors are required to review applicable administrative orders, policies, and procedures with the Human Resource Office and must complete appropriate forms to gain access to DFAS systems. New employees must meet with the Information Security (IS) Manager. The IS Manager is responsible for: (1) providing basic system security awareness training, (2) securing civilians’ and contractors’ signatures on an Automated Data Processing Security Awareness disclosure form, (3) identifying who an employees’ Terminal Area Security Officer (TASO) is and what the

TASO responsibilities are, and (4) notifying appropriate personnel when personnel actions occur. Those actions include providing access to or immediately terminating employee or contractor access to DFAS automated information system resources. The payroll offices and TSOPE facilities require a background check before a candidate can become an employee.

### *DISA DECC-MECH*

The security manager is responsible for processing and vetting new employees and contractors who are given access to DISA DECC-MECH facilities. All contractors and employees are required, at a minimum, to have a secret clearance and a positive National Agency Check. For employees, the security manager coordinates with the personnel office; and for contractors, the security manager coordinates with the contracting officer. For contractors, the security manager is responsible for confirming that all contractors are assigned to a valid contract, and have been approved to work at DISA DECC-MECH.

All new employees are required to sign DISA Form 312, “Classified Information Nondisclosure Agreement,” which serves as a nondisclosure agreement for sensitive and classified information. When employees are terminated, DISA requires them to sign the same Form 312 to confirm their understanding of the requirements placed upon them. New employees and contractors are required to complete a DD Form 2875, “System Authorization Access Request” to gain access to DISA systems. The security manager is responsible for vetting those forms and confirming that the person requesting access has the proper clearance for the level of access requested. For contractors, the security manager confirms the length of the contract and determines when system accounts should expire. All new employees and contractors must complete security awareness training.

## **C. Monitoring**

Management and supervisory personnel at DFAS and DISA monitor the performance quality and internal control environment as a normal part of their activities. DFAS and DISA have implemented a number of management, financial, and operational reports that help monitor the performance of payroll processing, as well as the DCPS system. These reports are reviewed periodically and action is taken as necessary. All procedural problems and exceptions to normal and scheduled processing are logged, reported, and resolved in a timely manner, with remedial action taken as necessary. In addition, several organizations within DoD perform monitoring activities associated with DCPS-related internal controls.

### **DISA Office of Inspector General**

The DISA OIG is an independent office within DISA that conducts internal audits, inspections, and investigations. DISA-related components that support DCPS are part of the DISA OIG audit universe and are subject to audits, inspections, and investigations conducted by this office.

## **Field Security Operations**

The Field Security Operations (FSO) conducts periodic System Readiness Reviews of DISA systems to determine whether those systems are in compliance with documented Standard Technical Implementation Guides (STIGs). The DCPS system components maintained by DISA are subject to FSO reviews. The FSO is independent of the DISA DECC-MECH management and does not maintain or configure DCPS.

## **DoD Office of Inspector General**

Congress established the DoD OIG under the Inspector General Act of 1978 to conduct and supervise audits and investigations related to DoD programs and operations. The DoD OIG reports directly to the Secretary of Defense and is independent of DFAS and DISA. DCPS is part of the DoD OIG audit universe and is subject to financial, operational, and information technology audits, reviews, and special assessment projects.

## **Certification and Accreditation**

DoD Instruction 5200.40, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, established a standard Department-wide process, set of activities, general tasks, and management structure to certify and accredit information systems that will maintain the information assurance and security posture of the Defense information infrastructure throughout the life cycle of each system. The certification process is a comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards to establish the extent to which a particular design and implementation meets specified security requirements and covers physical, personnel, administrative, information, information systems, and communications security. The accreditation process is a formal declaration by the designated approving authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

DCPS is subject to the requirements of DITSCAP and must meet all DITSCAP certification and accreditation requirements throughout its lifecycle. As part of the DCPS DITSCAP, DFAS and DISA have developed separate SSAAs for the DCPS application and for the system enclave within DISA that supports the application. Each SSAA is a living document that represents an agreement between the designated approving authority, certifying authority, user representative, and program manager. Among other items, the DCPS SSAA documents DCPS' mission description and system identification, environment description, system architecture description, system class, system security requirements, organizations and resources, and DITSCAP plan. On a periodic basis, the system security officer must verify and validate DCPS' compliance with the information in the SSAA by conducting vulnerability evaluations, security testing and evaluation, penetration testing, and risk management reviews. The DCPS application SSAA was issued on June 30, 2005, and is valid for three years. The DISA DECC-MECH enclave SSAA was issued on February 27, 2006, and is valid for three years. The DCPS application Authority to Operate (ATO), dated 29 July 2005, is on file with the

Information Assurance Manager. The DCPS ATO will be included in the annual Mechanicsburg Unclassified Enclave SSAA package update that is submitted to the DISA Designated Approval Authority (DAA).

## **D. Risk Assessment**

The DITSCAP, discussed in subsection C above, includes several activities that enable DFAS and DISA to assess risks associated with DCPS. The DCPS application and enclave SSAAs document threats to DCPS and its supporting technical environment. The SSAAs also contain residual risk assessments that document vulnerabilities noted during DCPS tests and analyses. The information contained in the SSAAs is updated on a periodic basis. Personnel from DFAS TSOPE and DISA DECC-MECH participate in risk assessment activities.

## **E. Information and Communication**

DCPS is the information system used to process civilian payroll for DoD and payroll customers from other Federal entities including the DoE, EPA, EOP, HHS, BBG, and VA. Payroll processing involving approximately 81 data files that interface with DCPS. Those interfaces are linked to other DoD financial systems, as well as external systems. The majority of the interfaces is automated and must conform to documented interface specifications developed by the TSOPE. The TSOPE is responsible for executing and monitoring all DCPS automated interfaces.

The support relationship between DFAS and DECC-MECH is documented through a service-level agreement that includes various DFAS and DECC-MECH points of contact and liaisons that should be used when DCPS issues arise. DECC-MECH has assigned a customer relationship manager to work with TSOPE to resolve any DCPS processing problems or concerns.

Directors and managers from TSOPE and the DISA DECC-MECH meet weekly to discuss DCPS processing issues. The Configuration Control Board; comprised of customer agencies, DISA DECC-MECH, TSOPE and payroll office personnel; review and approve functional and systemic changes to DCPS. The payroll offices have help desk functions to identify and track DCPS user issues and problems and communicate those issues and problems to DISA DECC-MECH for resolution.

## **F. Control Activities**

The DCPS control objectives and related control activities provided by the DoD OIG and approved by DFAS and DISA are included in Section III of this report, "Control Objectives, Control Activities, and Tests of Operating Effectiveness," to eliminate the redundancy that would result from listing them in this section and in Section III. Although the control objectives and related controls are included in Section III, they are nevertheless, an integral part of the description of controls.

## **G. User Organization Control Considerations**

DFAS and DISA control activities related to DCPS were designed with the assumption that certain controls would be placed in operation at user organizations. This section describes some of the controls that should be in operation at user organizations to complement the controls at DFAS and DISA.

User organizations should have policies and procedures in place to ensure that:

- the servicing payroll office is notified of all terminated employees with access to DCPS;
- the local Human Resource Office is notified of all terminated employees to ensure the employees are removed from the Master Employee Record in a timely manner;
- all time entered by timekeepers is approved and authorized by appropriate user organization management;
- all Master Employee Records created represent valid employees;
- all changes to the Master Employee Record are approved by appropriate user organization personnel prior to payroll processing;
- segregation of duties exists between those at the user organization who enter time and those who enter or change Master Employee Records;
- if a pseudo Social Security Number (SSN) is created, the pseudo SSN has been authorized by appropriate user organization personnel and, if necessary, is accurately tied to a primary and valid SSN;
- user organization managers review the “Control of Hours” and other payroll-related reports for appropriateness and accuracy;
- all invalid time entry interface feeds are reviewed and processed by appropriate user organization personnel in a controlled manner; and
- all invalid personnel record interface feeds are resolved in the interface system by user organization personnel with appropriate approval by user organization management.



---

**Section III: Control Objectives, Control Activities, and Tests  
of Operating Effectiveness**

---



### **III. Control Objectives, Control Activities, and Tests of Operating Effectiveness**

#### **A. Scope Limitations**

The control objectives documented in this section were specified by the DoD OIG. As described in Section II, DCPS interfaces with many systems. The controls described and tested in this section of the report are limited to those computer systems, operations, and processes directly related to DCPS itself. We did not perform any procedures to evaluate the integrity and accuracy of the data contained in DCPS. The controls related to the source and destination systems associated with the DCPS interfaces are specifically excluded from this review. In addition, we did not perform procedures to evaluate the effectiveness of data input, processing, and output controls within those interface systems. However, we did perform procedures to evaluate DCPS controls over data input from and output to the interfacing systems.

DFAS and DISA provided the Control Objective and Control Activity description columns. We populated the Tests Performed and Results of Testing columns. We conducted our audit for the purpose of forming an opinion on the description of the DCPS general and application controls at DFAS and DISA.

## B. Control Objectives, Control Activities, and Tests of Operating Effectiveness

### Application Control Objectives, Control Activities, Tests Performed, and Results of Testing

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
1.	<b>Physical Access</b>			
1	Controls prevent unauthorized physical access to DCPS data.	1.1 - Policies and procedures are documented to describe that personnel payroll records and other sensitive information is maintained and disposed of in accordance with Government-wide and agency-specific guidelines.	Inquired with appropriate personnel and scan policies and procedures to confirm that personnel payroll records and other sensitive information is maintained and disposed of in accordance with Government-wide and agency-specific guidelines.  [All payroll offices]	<u>DFAS Indianapolis:</u> Documented policies and procedures for the physical security were not in place.  <u>DFAS Cleveland:</u> No relevant exceptions noted.
1.2 - All documents and storage media are stored in physically and environmentally secure containers.		Confirmed through corroborative inquiry and inspection of storage process documentation that documents and storage media are stored properly in environmentally secure containers.  [All payroll offices]	<u>DFAS Indianapolis:</u> We noted payroll processing locations were not physically secured. In addition, file cabinets containing payroll information were not secured.  <u>DFAS Cleveland:</u> No relevant exceptions noted.	
1.3 - All visitors to the payroll office must sign in and out with the authorized security personnel.		Inquired with appropriate personnel and obtained and inspected a sample of visitor logs from the payroll office to confirm that visitors must sign-in with authorized security personnel.	<u>DFAS Indianapolis:</u> A visitor access process was in place at DFAS Indianapolis; however, individuals do not wear	

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			[All payroll offices]	<p>badges that identify them as visitors, and we did not receive visitor logs.</p> <p><u>DFAS Cleveland:</u></p> <p>We noted the following for visitor access testing:</p> <ul style="list-style-type: none"> <li>• 1 of 22 sample of dates tested did not have the visited organization on the visitor badge log,</li> <li>• 4 of 22 sample of dates tested did not have the authorized sponsor on visitor logs,</li> <li>• 1 of 22 sample of dates tested did not have the reason for the visit on the visitor logs,</li> <li>• 1 of 22 sample of dates tested did not have the floor visited on the visitor badge log, and</li> <li>• 1 of 22 sample of dates tested did not have the visitor badge turn-in date on the visitor badge log.</li> </ul>
		1.4 - All terminals and payroll records are located in physically secured locations.	Confirmed through corroborative inquiry with appropriate personnel that the terminal rooms are physically secure.	<p><u>DFAS Indianapolis:</u></p> <p>We noted physically unsecured payroll processing locations. In</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			[All payroll offices]	<p>addition, we noted unsecured file cabinets that stored payroll information.</p> <p><u>DFAS Cleveland:</u></p> <p>No relevant exceptions noted.</p>
		1.5 - Users dispose of personnel and payroll records in accordance with Government-wide and agency-specific guidelines.	<p>Confirmed through corroborative inquiry with appropriate personnel that payroll records are disposed of using destruction bins in accordance with Government-wide and agency-specific guidelines.</p> <p>[All payroll offices]</p>	No relevant exceptions noted.
		1.6 - Each terminal automatically disconnects from the system when not used after a specified period of time.	<p>Confirmed through corroborative inquiry with appropriate personnel that each terminal automatically disconnects from the system when not used after a specified period of time.</p> <p>[All payroll offices]</p>	No relevant exceptions noted.
		1.7 - When terminals are not in use, terminal rooms are locked, or the terminals are can be secured.	<p>Confirmed through corroborative inquiry with appropriate personnel that when terminals are not in use, terminal rooms are locked, or the terminals can be secured.</p> <p>[All payroll offices]</p>	No relevant exceptions noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
2	<b>System Access</b>			
2	Controls prevent unauthorized system access to DCPS data.	<p>2.1 - The ability to view, modify, or transfer information contained in the payroll master files is restricted to authorized personnel.</p> <p>Each operator is required to have a completed and authorized authorization form before being granted access to the system.</p> <p>Authorization profiles of users limit what transactions data entry personnel can enter.</p>	<p>Inquired with appropriate personnel and inspected a random sample of SAARs to confirm the following.</p> <ul style="list-style-type: none"> <li>• The payroll master file and output is restricted to authorized personnel.</li> <li>• Each operator has authorization before being granted access to the system.</li> <li>• User profiles limit the type of transaction data entry personnel can enter into DCPS.</li> </ul> <p>[All payroll offices]</p>	<p><u>DFAS Indianapolis:</u></p> <p><i>Non-payroll users</i></p> <p>DFAS was unable to provide 11 of 45 selected non-payroll user access forms.</p> <p>We noted the following for the 34 non-payroll user access forms provided:</p> <ul style="list-style-type: none"> <li>• 6 of 34 non-payroll user forms indicated a user type that did not match the user type in DCPS.</li> <li>• 2 of 34 non-Payroll user forms indicated authorization types that did not match the user type in the list of DCPS users.</li> <li>• 7 of 34 non-payroll user forms were missing the DCPS Security Awareness training completion date.</li> <li>• 1 of 34 non-payroll user access forms was missing the user's</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>signature.</p> <ul style="list-style-type: none"> <li>• 1 of 34 non-payroll user access forms was missing the supervisor's signature.</li> <li>• 5 of 34 non-payroll user access forms were missing the date of the supervisor's approval.</li> <li>• 13 of 34 non-payroll user access forms were missing the security manager's signature.</li> <li>• 14 of 34 non-payroll user access forms were missing the date of the security manager's approval.</li> <li>• 7 of 34 non-payroll user access requests were processed using the incorrect form. Users obtained access using the DCPS Security Access Questionnaire.</li> </ul> <p><i>Payroll users</i></p> <p>DFAS was unable to provide 5 of 45 selected payroll user access forms.</p>



No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>We noted the following for the 40 payroll user access forms provided:</p> <ul style="list-style-type: none"> <li>• 13 of 40 payroll users did not complete the correct form. Users obtained access using non-payroll user access forms.</li> <li>• 17 of 40 payroll user access forms indicated a user type that did not match the user type listed in DCPS.</li> <li>• 6 of 40 payroll user access forms were missing the DCPS Security Awareness training completion date.</li> <li>• 3 of 40 payroll user access forms were missing the date of the supervisor's signature.</li> <li>• 5 of 40 payroll user access forms were missing the security manager's signature.</li> <li>• 7 of 40 payroll user access forms were</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>missing the date of the security manager's approval.</p> <ul style="list-style-type: none"> <li>• 4 of 40 payroll user access request were processed using the incorrect form. Users obtained access using the DCPS Security Access Questionnaire.</li> </ul> <p><u>DFAS Cleveland:</u> <i>Non-payroll users</i></p> <p>DFAS was unable to provide 4 of 45 selected non-payroll user access forms.</p> <p>We noted the following for the 41 non-payroll user access forms provided:</p> <ul style="list-style-type: none"> <li>• 5 of 41 non-payroll user forms indicated a user type that did not match the user type in DCPS.</li> <li>• 4 of 41 non-payroll user forms indicated authorization types that did not match the authorization type in DCPS.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<ul style="list-style-type: none"> <li>• 9 of 41 non-payroll user forms were missing the DCPS Security Awareness training completion date.</li> <li>• 1 of 41 non-payroll user access forms was missing the supervisor's signature.</li> <li>• 5 of 41 non-payroll user access forms were missing the date of the supervisor's approval.</li> <li>• 10 of 41 non-payroll user access forms were missing the security manager's signature.</li> <li>• 13 of 41 non-payroll user access forms were missing the date of the security manager's approval.</li> <li>• 6 of 41 non-payroll user access requests were processed using the incorrect form. Users obtained access using the DCPS Security Access Questionnaire.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p><i>Payroll users</i></p> <p>DFAS was unable to provide 5 of 45 selected payroll user access forms.</p> <p>We noted the following for the 40 Payroll user access forms provided:</p> <ul style="list-style-type: none"> <li>• 14 of 40 payroll user forms indicated a user type that did not match the user type listed in DCPS.</li> <li>• 5 of 40 payroll user forms were missing the user DCPS Security Awareness training completion date.</li> <li>• 1 of 40 payroll user access forms was missing the user's signature.</li> <li>• 3 of 40 payroll user access forms were missing the date of the supervisor's approval.</li> <li>• 5 of 40 payroll user access forms were missing the security manager's signature.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<ul style="list-style-type: none"> <li>• 8 of 40 payroll user access forms were missing the date of the security manager's approval.</li>   <li>• 12 of 40 payroll access request forms were processed using the incorrect non-payroll user form for payroll user type access.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		<p>2.2 - Policies and procedures are documented to describe how application users are appropriately identified and authenticated. Access to the application and output is restricted to authorized users for authorized purposes.</p>	<p>Inquired with appropriate personnel and inspected policies and procedures to confirm that users are appropriately identified and authenticated and that access to the application and output is restricted to authorized users for authorized purposes.</p> <p>[All payroll offices]</p>	<p>No relevant exceptions noted.</p>
		<p>2.3 - On-line access logs are maintained by the System Management Office and are reviewed regularly for unauthorized access attempts.</p>	<p>Inquired with appropriate personnel and inspected access logs and e-mails for unauthorized access attempts to confirm that logs are maintained by the System Management Office and are reviewed regularly for unauthorized access attempts.</p> <p>[All payroll offices]</p>	<p>No relevant exceptions noted.</p>
		<p>2.4 - Remote terminal connections are secured and connected through Government-issued computers.</p>	<p>Inquired with appropriate personnel and inspected remote terminal connections to confirm that they are secured and are connected through Government computers.</p> <p>Obtained a complete listing of all new DFAS Civilian Pay users with remote access from 10/1/2007 to 3/31/2008. Selected a sample of users and obtained the remote access packages to confirm that it included a:</p>	<p>No relevant exceptions noted.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			<ul style="list-style-type: none"> <li>• Remote User Access Request Form and associated approvals and</li> <li>• Memorandum of Agreement</li> </ul> [All payroll offices]	
		2.5 - Data entry terminals are connected to the system only during specified periods of the day, which correspond with the business hours of the data entry personnel.	Confirmed through corroborative inquiry with appropriate personnel that terminals are not authorized to be connected after business hours.  [All payroll offices]	<u>DFAS Indianapolis:</u> We noted no physical security controls in place to restrict after business hours access to the terminals.  <u>DFAS Cleveland:</u> No relevant exceptions noted.
		2.6 - User IDs and passwords are required to gain access to the DCPS application.	Confirmed through corroborative inquiry with appropriate personnel and inspected the DCPS log-in screen to confirm that user IDs and passwords are required to gain access to the DCPS application.  [All payroll offices]	No relevant exceptions noted.
<b>3</b>	<b>Restricted Access</b>			
3	Controls provide reasonable assurance that DCPS	3.1 - The detailed 592 Reconciliation shows all pertinent data describing	Inquired with appropriate personnel and inspected a random sample of 592	<u>DFAS Indianapolis:</u>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
	authorized users are restricted to access only areas needed to complete their assigned responsibilities, and controls maintain segregation of duties.	that the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and related balances are reconciled in the appropriate accounting period to corresponding general ledger accounts within DCPS. All reconciling items are investigated and cleared in a timely manner by supervisory personnel, prior to disbursement.	<p>Reconciliations for each database to confirm the following:</p> <ul style="list-style-type: none"> <li>• The detailed payroll reconciliation shows pertinent data describing that the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and related balances are reconciled in the appropriate accounting period to corresponding general ledger accounts within DCPS.</li> <li>• Each 592 Reconciliation is approved by management prior to disbursement.</li> <li>• Reconciling items are investigated and cleared in a timely manner by supervisory personnel, prior to disbursement.</li> </ul> <p>[All payroll offices]</p>	<p>DFAS was unable to provide 8 of 45 592 Reconciliations requested.</p> <ul style="list-style-type: none"> <li>• 1 of 45 592 Reconciliations did not balance and did not have a supplemental 592 Reconciliation prepared.</li> <li>• 1 of 45 592 Reconciliations did not contain a signed report of withholdings.</li> </ul> <p><u>DFAS Cleveland:</u> No relevant exceptions noted.</p>
		3.2 - Summary payroll reports including Online Queries (OLQs) of total disbursements, Retirement, TSP, Bonds, and other withholdings are reviewed and approved by management prior to disbursement.	<p>Inquired with appropriate personnel and inspected summary reports and OLQs reviewed and approved by management prior to disbursement.</p> <p>[All payroll offices]</p>	<p><u>DFAS Indianapolis:</u> <i>592 Reconciliations</i> DFAS personnel used the 592 Balancing Desk Guide; however, a policy regarding document retention was not in place. Specifically, there was no</p>



No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>requirement to retain the printed and reviewed report checklist or the signed Report of Withholdings.</p> <p><i>Management Summary Reports</i></p> <p>No policy was in place that required a complete and accurate listing of management summary reports generated and reviewed by Civilian Pay Processing Personnel.</p> <p>DFAS was unable to provide the Separation Actions without Separations Codes Desk Guide.</p> <p>The Less than \$1 Over \$5,000 Desk Guide did not have an increased threshold amount of \$10,000 in the review procedures.</p> <p><u>DFAS Cleveland:</u></p> <p><i>DD 592 Reconciliations</i></p> <p>DFAS personnel used the Balancing Desk Guide; however, a policy</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>regarding document retention was not in place. Specifically, there was no requirement to retain the printed and reviewed report checklist or the signed Report of Withholdings.</p> <p><i>Management Summary Reports</i></p> <p>No policy was in place that required a complete and accurate listing of management summary reports generated and reviewed by Civilian Pay Processing personnel</p> <p>DFAS was unable to provide the Desk Guides for the following critical reports:</p> <ul style="list-style-type: none"> <li>• Separation Action without Separation Codes Desk Guide,</li> <li>• Dual SSN/Mongoose Desk Guide, and</li> <li>• P6702R01 - Invalid SSN/Deceased Employees/Negative Year-To-Date Desk Guide.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
<b>4</b>	<b>System and Software Changes</b>			
4	Controls provide reasonable assurance that system and software changes are authorized, effectively and efficiently implemented, tested, and documented. (General Computer controls only)	Not applicable as this is tested by the General Computer Controls. Please see control objectives 13.1-13.6	Not Applicable as this is tested by the General Computer Controls. Please see control objectives 13.1-13.6	Not Applicable as this is tested by the General Computer Controls. Please see control objectives 13.1-13.6
5	[ This control objective was intentionally left blank]			
<b>6</b>	<b>Enterprise-Wide Security Program</b>			
6	Controls include an enterprise-wide security program to review and manage risks and ensure that policies comply with laws and regulations.	6.1 - A Security Program has been prepared specific to payroll operations and is approved by management. The plan is regularly tested and updated to reflect the results of such tests.	Inquired with appropriate personnel to confirm a Security Program for payroll operations exists. Obtained and inspected the date of the plans and corroborated with management that these plans are current, contain up-to-date information, and are readily available to all relevant personnel. Inquired with management to confirm that the plans have been approved.  [All payroll offices]	No relevant exceptions noted.
<b>7</b>	<b>Personnel and Payroll Data</b>			
7	Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA	7.1 - Policies and procedures are documented to describe that only valid and accurate changes are made to the payroll master files and payroll	Inquired with appropriate personnel and inspected policies and procedures to confirm that only valid changes are made to the payroll master files and	No relevant exceptions noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
	General Computer Control locations are valid, accurate and authorized, complete, and timely, and support financial reporting requirements, and provide sufficient audit trails.	withholding tables.	payroll withholding tables.  [All payroll offices]	
		7.2 - Programmed validation and edit checks identify erroneous data.	Inquired with appropriate personnel and observed programmed validation and edit checks to confirm that they identify erroneous data entered directly into DCPS.  [All payroll offices]	No relevant exceptions noted.
		7.3 - The ability to view, modify, or transfer information contained in the payroll master files is restricted to authorized personnel.	Inquired with appropriate personnel and inspected a random sample of SAARs to confirm the following. <ul style="list-style-type: none"> <li>• The payroll master file and output is restricted to authorized personnel.</li> <li>• Each operator is authorized before being granted access to the system.</li> <li>• Confirm user profiles limit the type of transactions data entry personnel can enter into DCPS.</li> </ul> [All payroll offices]	<u>DFAS Indianapolis:</u> <i>Non-payroll users</i> DFAS was unable to provide 11 of 45 selected non-payroll user access forms. We noted the following for the 34 non-payroll user access forms provided: <ul style="list-style-type: none"> <li>• 6 of 34 non-payroll user forms indicated a user type that did not match the user type in DCPS.</li> <li>• 7 of 34 non-payroll user forms were missing the DCPS Security Awareness</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>training completion date.</p> <ul style="list-style-type: none"> <li>• 2 of 34 non-payroll user forms indicated a user type that did not match the user type in DCPS.</li> <li>• 1 of 34 non-payroll user access forms was missing the user's signature.</li> <li>• 1 of 34 non-payroll user access forms was missing the supervisor's signature.</li> <li>• 5 of 34 non-payroll user access forms were missing the date of the supervisor's approval.</li> <li>• 13 of 34 non-payroll user access forms were missing the security manager's signature.</li> <li>• 14 of 34 non-payroll user access forms were missing the date of the security manager's approval.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<ul style="list-style-type: none"> <li>• 7 of 34 non-payroll user access requests were processed using the incorrect form. User obtained access using the DCPS Security Access Questionnaire.</li> </ul> <p><i>Payroll users</i></p> <p>DFAS was unable to provide 5 of 45 selected payroll user access forms.</p> <p>We noted the following for the 40 payroll user access forms provided:</p> <ul style="list-style-type: none"> <li>• 13 of 40 payroll user access forms were the incorrect form. Users obtained access using non-payroll user access forms.</li> <li>• 17 of 40 payroll user access forms indicated user types that did not match the user type in listed in DCPS.</li> <li>• 6 of 40 payroll user access forms were missing the DCPS Security Awareness completion date.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<ul style="list-style-type: none"> <li>• 3 of 40 payroll user access forms were missing the date of the supervisor's signature.</li> <li>• 5 of 40 payroll user access forms were missing the Security manager's signature.</li> <li>• 7 of 40 payroll user access forms were missing the date of the security manager's approval.</li> <li>• 4 of 40 payroll user access forms processed were incorrect forms. Users obtained access using the DCPS Security Questionnaire.</li> </ul> <p><u>DFAS Cleveland:</u>  <i>Non-payroll users</i>  DFAS was unable to provide 4 of 45 selected non-payroll user access forms.</p> <p>We noted the following for the 41 non-payroll user access forms provided:</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<ul style="list-style-type: none"> <li>• 5 of 41 non-payroll user forms indicated a user type that did not match the user type in DCPS.</li> <li>• 4 of 41 non-payroll user forms indicated authorization types that did not match the authorization type in DCPS.</li> <li>• 9 of 41 non-payroll user forms were missing the completion date for the DCPS Security Awareness training.</li> <li>• 1 of 41 non-payroll user access forms was missing the supervisor's signature.</li> <li>• 5 of 41 non-payroll user access forms were missing the date of the supervisor's approval.</li> <li>• 10 of 41 non-payroll user access forms were missing the security manager's signature.</li> <li>• 13 of 41 non-payroll user access forms were</li> </ul>



No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>missing the date of the security manager's approval.</p> <ul style="list-style-type: none"> <li>• 6 of 41 non-payroll user access forms were the incorrect form. The user obtained access using the DCPS Security Access Questionnaire.</li> </ul> <p><i>Payroll users</i></p> <p>DFAS was unable to provide 5 of 45 selected Payroll user access forms.</p> <p>We noted the following for the 40 payroll user access forms provided:</p> <ul style="list-style-type: none"> <li>• 14 of 40 payroll user forms indicated a user type that did not match the user type listed in DCPS.</li> <li>• 5 of 40 payroll user forms were missing the DCPS Security Awareness training completion date.</li> <li>• 1 of 40 payroll user access forms did not include the user's signature.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<ul style="list-style-type: none"> <li>• 3 of 40 payroll user access forms were missing the date of the supervisor's approval.</li> <li>• 5 of 40 payroll user access forms were missing the security manager's signature.</li> <li>• 10 of 40 payroll user access forms were missing the date of the security manager's approval.</li> <li>• 2 of 40 forms processed were the incorrect form.</li> <li>• 12 of 40 selected payroll user access forms were processed using the incorrect non-payroll user form.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		<p>7.4 - Changes to the payroll withholding tables and master files are compared to authorized source documents by supervisory personnel to ensure that they were input accurately.</p>	<p>Inquired with appropriate personnel and inspected documentation regarding the process of tax changes to the payroll withholding tables and master files being compared to authorized source documents by supervisory personnel to confirm that they were reviewed and approved.</p> <p>Inquired with appropriate personnel and inspected the Imaging process to confirm that inputs are compared to authorized Imaging source documents and input accurately.</p> <p>[Indianapolis payroll office]</p>	<p>No relevant exceptions noted.</p>
		<p>7.5 - The system provides an audit trail of all transactions processed, transaction errors, error descriptions, and error correction procedures. Audit trails are reviewed by supervisory personnel and erroneous data are captured, reported, investigated, and corrected.</p>	<p>Inquired with appropriate personnel and inspected audit trails of transactions to confirm that erroneous transactions are reviewed by supervisory personnel, and captured, reported, investigated, and corrected.</p> <p>[Pensacola TSO]</p>	<p>No relevant exceptions noted.</p>
		<p>7.6 - Policies and procedures are documented to describe that transactions from interfacing systems are subjected to the payroll system edits, validations, and error-correction procedures.</p>	<p>Inquired with appropriate personnel and inspected policies and procedures to confirm that transactions from interfacing systems are subjected to the payroll system edits, validations, and error-correction procedures.</p> <p>[Pensacola TSO]</p>	<p>No relevant exceptions noted.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		7.7 - Policies and procedures are documented to describe that changes made to the payroll master files and withholding tables are authorized, input, and processed timely.	Inquired with appropriate personnel and inspected policies and procedures to confirm that changes to the payroll master files and withholding tables are authorized, input, and processed timely.  [Cleveland payroll office]	No relevant exceptions noted.
		7.8 - Policies and procedures are documented to describe that changes made to the payroll master files and withholding tables are authorized, input, and processed timely.	Inquired with appropriate personnel and inspected policies and procedures to confirm that changes to the payroll master files and withholding tables are authorized, input, and processed timely.  [Indianapolis payroll office]	No relevant exceptions noted.
		7.9 - Changes to the payroll master file and withholding table data are logged in numerous reports and reviewed by supervisory personnel to ensure that all requested changes are processed timely.	Inquired with appropriate personnel and inspected management summary reports to confirm that changes to the payroll master file and table data are logged and reviewed by supervisory personnel.  [All payroll offices]	<u>DFAS Indianapolis:</u> <i>Management Summary Reports</i>  The management summary reports for the audit period were not available; therefore, no tests were performed.  DFAS was unable to provide the Separation Actions without Separations Codes Desk Guide.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>The Less than \$1 Over \$5,000 Desk Guide did not have an increased threshold amount of \$10,000 in the review procedures.</p> <p><u>DFAS Cleveland:</u> <i>Management Summary Reports</i></p> <p>The management summary reports for the audit period were not available; therefore, no tests were performed.</p> <p>DFAS was unable to provide the following Desk Guides for the following critical reports:</p> <ul style="list-style-type: none"> <li>• Separation Action without Separation Codes Desk Guide,</li> <li>• Dual SSN/Mongoose Desk Guide, and</li> <li>• P6702R01 - Invalid SSN/Deceased Employees/Negative Year-To-Date Desk Guide.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		<p>7.10 - Requests to change the payroll master file data and withholding table are submitted on pre-numbered Remedy Tickets; the numerical sequence of the Remedy Tickets is accounted for to ensure that the requested changes are processed timely; access to source documents is controlled; and key source documents require signatures from supervisory personnel.</p>	<p>Inquired with appropriate personnel and inspected a random sample of Remedy Tickets to confirm that the:</p> <ul style="list-style-type: none"> <li>• requests were pre-numbered;</li> <li>• sequence was accounted for so that the forms were accounted for timely;</li> <li>• tickets were processed in a timely manner; and</li> <li>• access to the source documents was controlled.</li> </ul> <p>[All payroll offices]</p>	<p><u>DFAS Indianapolis:</u> 4 of 45 Remedy Tickets were not resolved within the required DFAS Indianapolis processing schedule.</p> <p><u>DFAS Cleveland:</u> No relevant exceptions noted.</p>
		<p>7.11 - Payroll master file data and withholding table data are edited and validated and errors identified on the Personnel Interface Invalid Report are corrected promptly.</p>	<p>Inquired with appropriate personnel and inspected a sample of Personnel Interface Invalid Reports of erroneous transactions to confirm that items are investigated and resolved.</p> <p>[All payroll offices]</p>	<p><u>DFAS Indianapolis:</u> DFAS was unable to provide 12 of 45 PIIRs requested.</p> <p>We noted the following for the remaining 33 PIIRs:</p> <ul style="list-style-type: none"> <li>• 3 of 33 PIIRs did not include annotations using the proper standard codes.</li> <li>• 2 of 33 PIIRs did not include the dates the payroll technician addressed the errors.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p><u>DFAS Cleveland:</u></p> <p>DFAS was unable to provide 16 of 45 PIIRs requested.</p> <p>We noted the following for the remaining 29 PIIR;</p> <ul style="list-style-type: none"> <li>• 1 of 29 available PIIRs was missing the payroll technician's signature.</li> <li>• 1 of 29 PIIRs did not include the date the payroll technician annotated the report.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		<p>7.12 - Policies and procedures are documented to describe that payroll processing is accurate and recorded in the proper period.</p>	<p>Inquired with appropriate personnel and inspected policies and procedures to confirm that payroll processing is accurate and recorded in the appropriate period.</p> <p>[All payroll offices]</p>	<p><u>DFAS Indianapolis:</u></p> <p><i>592 Reconciliations</i></p> <p>DFAS personnel use the 592 Balancing Desk Guide; however, a policy regarding document retention was not in place. Specifically, there was no requirement to retain the printed and reviewed report checklist or the signed Report of Withholdings.</p> <p><i>Management Summary Reports</i></p> <p>The management summary reports for the audit period were not available; therefore, no tests were performed.</p> <p>DFAS was unable to provide the Separation Actions without Separations Codes Desk Guide.</p> <p>The Less than \$1 Over \$5,000 Desk Guide did not have an increased threshold amount of \$10,000 in the review</p>



No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>procedures.</p> <p><u>DFAS Cleveland:</u></p> <p><i>592 Reconciliations</i></p> <p>DFAS personnel use the 592 Balancing Desk Guide; however, a policy regarding document retention was not in place. Specifically, there was no requirement to retain the printed and reviewed report checklist or the signed Report of Withholdings.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p><i>Management Summary Reports</i></p> <p>The management summary reports for the audit period were not available; therefore, no tests were performed.</p> <p>DFAS was unable to provide the Desk Guides for the following critical reports:</p> <ul style="list-style-type: none"> <li>• Separation Action without Separation Codes Desk Guide,</li> <li>• Dual SSN/Mongoose Desk Guide, and</li> <li>•</li> <li>• P6702R01 - Invalid SSN/Deceased Employees/Negative Year-To-Date Desk Guide.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		<p>7.13 - Compliance with the payroll disbursement processing schedule is monitored by management.</p>	<p>Inquired with appropriate personnel and inspected pay processing schedules and the payroll disbursement process to confirm the monitoring of payroll disbursement processing schedule by management.</p> <p>Inspected a random sample of 592 reconciliations to confirm that payroll disbursement is approved and monitored by management.</p> <p>[All payroll offices]</p>	<p><u>DFAS Indianapolis:</u></p> <p><i>592 Reconciliations</i></p> <p>DFAS personnel used the 592 Balancing Desk Guide; however, a policy regarding document retention was not in place. Specifically, there was no requirement to retain the printed and reviewed report checklist or the signed Report of Withholdings.</p> <p>DFAS was unable to provide 8 of 45 reconciliations that provided evidence of reconciliation, final review, and disbursement of payroll.</p> <p><i>Management Summary Reports</i></p> <p>The management summary reports for the audit period were not available; therefore, no tests were performed.</p> <p>DFAS was unable to provide the Separation Actions without</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>Separations Codes Desk Guide.</p> <p>The Less than \$1 Over \$5,000 Desk Guide did not have an increased threshold amount of \$10,000 in the review procedures.</p> <p><u>DFAS Cleveland:</u></p> <p><i>592 Reconciliations</i></p> <p>DFAS personnel use the 592 Balancing Desk Guide; however, a policy regarding document retention was not in place. Specifically, there was no requirement to retain the printed and reviewed report checklist or the signed Report of Withholdings.</p> <p>10 of 45 selected reconciliations were missing documentation of a final disbursement authorization.</p> <p><i>Management Summary Reports</i></p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>The management summary reports for the audit period were not available; therefore, no tests were performed.</p> <p>DFAS was unable to provide the Desk Guides for the following critical reports:</p> <ul style="list-style-type: none"> <li>• Separation Action without Separation Codes Desk Guide,</li> <li>• Dual SSN/Mongoose Desk Guide, and</li> <li>• P6702R01 - Invalid SSN/Deceased Employees/Negative Year-To-Date Desk Guide.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		<p>7.14 - The detailed 592 payroll reconciliation shows all pertinent data describing the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and the related balances are reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS. All reconciling items are investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.</p>	<p>Inquired with appropriate personnel and inspected a random sample of 592 Reconciliations for each database to confirm:</p> <ul style="list-style-type: none"> <li>• the detailed payroll reconciliation shows pertinent data describing the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and the related balances are reconciled in the appropriate accounting period to corresponding general ledger accounts within DCPS;</li> <li>• each 592 Reconciliation is approved by management prior to disbursement; and</li> <li>• reconciling items are investigated and cleared on a timely basis by supervisory personnel prior to disbursement.</li> </ul> <p>[All payroll offices]</p>	<p><u>DFAS Indianapolis:</u> DFAS was unable to provide 8 of 45 reconciliations requested. Of the remaining 32 592 reconciliations:</p> <ul style="list-style-type: none"> <li>• 1 592 reconciliation did not balance, and a supplemental was not prepared; and</li> <li>• 1 592 reconciliation did not contain a signed report of withholdings.</li> </ul> <p><u>DFAS Cleveland:</u> 10 out of 45 reconciliations did not contain a final disbursement authorization.</p>
		<p>7.15 - Summary payroll reports including OLQs of total disbursements, Retirement, TSP, Bonds, and other withholdings are periodically reviewed by supervisory personnel for accuracy and ongoing pertinence of the payroll master file and withholding tables, and approved</p>	<p>Inquired with appropriate supervisor and management personnel, obtained and inspected management summary payroll reports or OLQs to confirm the following:</p> <ul style="list-style-type: none"> <li>• Payroll master files and withholding tables are periodically reviewed by</li> </ul>	<p><u>DFAS Indianapolis:</u> <i>592 Reconciliations</i> DFAS personnel used the 592 Balancing Desk Guide however, a policy regarding document retention was not in place.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		by management prior to disbursement.	<p>supervisory personnel for accuracy and ongoing pertinence; and</p> <ul style="list-style-type: none"> <li>• Reports are approved by management prior to disbursement.</li> </ul> <p>[All payroll offices]</p>	<p>Specifically, there was no requirement to retain the printed and reviewed report checklist or the signed Report of Withholdings.</p> <p><i>Management Summary Reports</i></p> <p>The management summary reports for the audit period were not available; therefore, no tests were performed.</p> <p>DFAS was unable to provide the Separation Actions without Separations Codes Desk Guide.</p> <p>The Less than \$1 Over \$5,000 Desk Guide did not have an increased threshold amount of \$10,000 in the review procedures.</p> <p><u>DFAS Cleveland:</u></p> <p><i>592 Reconciliations</i></p> <p>DFAS personnel used the 592 Balancing Desk Guide; however, a policy regarding document</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>retention was not in place. Specifically, there was no requirement to retain the printed and reviewed report checklist or the signed Report of Withholdings.</p> <p><i>Management Summary Reports</i></p> <p>The management summary reports for the audit period were not available; therefore, no tests were performed.</p> <p>DFAS was unable to provide the Desk Guides for the following critical reports:</p> <ul style="list-style-type: none"> <li>• Separation Action without Separation Codes Desk Guide,</li> <li>• Dual SSN/Mongoose Desk Guide, and</li> <li>• P6702R01 - Invalid SSN/Deceased Employees/Negative Year-To-Date Desk Guide.</li> </ul>



No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		<p>7.16 - Policies and procedures are documented to describe that disbursed payroll (including compensation and withholding) is accurately calculated and recorded.</p>	<p>Inquired with appropriate personnel and inspected policies and procedures to confirm controls are in place to monitor that disbursed payroll is accurately calculated and recorded.</p> <p>[All payroll offices]</p>	<p><u>DFAS Indianapolis:</u>  <i>592 Reconciliations</i></p> <p>DFAS personnel used the 592 Balancing Desk Guide; however, a policy regarding document retention was not in place. Specifically, there was no requirement to retain the printed and reviewed report checklist or the signed Report of Withholdings.</p> <p><i>Management Summary Reports</i></p> <p>The management summary reports for the audit period were not available; therefore, no tests were performed.</p> <p>DFAS was unable to provide the Separation Actions without Separations Codes Desk Guide.</p> <p>The Less than \$1 Over \$5,000 Desk Guide did not include an increased threshold amount of \$10,000 within its review</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>procedures.</p> <p><u>DFAS Cleveland:</u></p> <p><i>592 Reconciliations</i></p> <p>DFAS personnel used the 592 Balancing Desk Guide; however, a policy regarding document retention was not in place. Specifically, there was no requirement to retain the printed and reviewed report checklist or the signed Report of Withholdings.</p> <p><i>Management Summary Reports</i></p> <p>The management summary reports for the audit period were not available; therefore, no tests were performed.</p> <p>DFAS was unable to provide the Desk Guides for the following critical reports:</p> <ul style="list-style-type: none"> <li>• Separation Action without Separation Codes Desk Guide,</li> <li>• Dual SSN/Mongoose Desk Guide, and</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<ul style="list-style-type: none"> <li>P6702R01 - Invalid SSN/Deceased Employees/Negative Year-To-Date Desk Guide.</li> </ul>
		<p>7.17 - DCPS performs limit and reasonableness checks on employee earnings.</p>	<p>Inquired with appropriate personnel and inspected a limit and reasonableness management summary report to confirm the required limit and reasonableness checks are performed on employee earnings.</p> <p>[All payroll offices]</p>	<p><u>DFAS Indianapolis:</u> <i>Management Summary Reports</i></p> <p>The management summary reports for the audit period were not available; therefore, no tests were performed.</p> <p>DFAS was unable to provide the Separation Actions without Separations Codes Desk Guide.</p> <p>The Less than \$1 Over \$5,000 Desk Guide did not have an increased threshold amount of \$10,000 in the review procedures.</p> <p><u>DFAS Cleveland:</u> <i>Management Summary Reports</i></p> <p>The management summary</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>reports for the audit period were not available; therefore, no tests were performed.</p> <p>DFAS was unable to provide the Desk Guides for the following critical reports:</p> <ul style="list-style-type: none"> <li>• Separation Action without Separation Codes Desk Guide,</li> <li>• Dual SSN/Mongoose Desk Guide, and</li> <li>• P6702R01 - Invalid SSN/Deceased Employees/Negative Year-To-Date Desk Guide.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		7.18 - Policies and procedures are documented to describe that only valid, authorized employees are paid and that payroll is disbursed to appropriate employees.	<p>Inquired with appropriate personnel and inspected policies and procedures to confirm that only valid, authorized employees are paid and that payroll is disbursed to appropriate employees.</p> <p>[All payroll offices]</p>	No relevant exceptions noted.
		7.19 - Supervisory personnel periodically review listings, such as the Personnel/Payroll Reconciliation Report, of current employees within each user organization and notify the corresponding user organization's personnel department of necessary changes.	<p>Inquired with appropriate personnel and inspected the Personnel/Payroll Reconciliation Report to confirm it was sent to management for review of employee listings and notification.</p> <p>Obtained and inspected a sample of Personnel/Payroll Reconciliation Reports, along with the corresponding supervisor document log, to confirm that personnel or payroll items that require resolution are investigated and resolved by the appropriate Civilian Pay personnel.</p> <p>[All payroll offices]</p>	<p><u>DFAS Indianapolis:</u></p> <p>No policy was in place that required review annotations and document retention for the personnel/payroll reports.</p> <p>DFAS was unable to provide 4 of 45 Personnel/Payroll Reconciliation Report reviews requested.</p> <p>We noted 8 of 41 reports did not include notification sent to the user agency with the necessary changes.</p> <p><u>DFAS Cleveland:</u></p> <p>No Personnel/Payroll Reconciliations were prepared during the testing period.</p> <p>No policy was in place that required review</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>annotations and document retention for the Personnel/Payroll Reports.</p>
		<p>7.20 - Only authorized personnel have the ability to disburse payroll.</p>	<p>Inquired with the appropriate personnel and inspected the policies and procedures regarding the disbursement of payroll, and inspected a sample of DCPS user profiles to confirm that only authorized personnel have the ability to disburse payroll.</p> <p>[DFAS Saufley Field]</p>	<p><u>DFAS Saufley Field:</u> 1 of 66 SAARs tested included a justification for access that did not include the responsibility to disburse payroll.</p>
		<p>7.21 - Policies and procedures are documented to describe that controls provide reasonable assurance of the integrity and reliability of DCPS data for financial reporting purposes.</p>	<p>Inquired with appropriate personnel and inspected policies and procedures to confirm that the 592 Reconciliations are used by payroll office personnel to provide assurance of the integrity and reliability of DCPS data for financial reporting purposes.</p> <p>[All payroll offices]</p>	<p><u>DFAS Indianapolis:</u> <i>592 Reconciliations</i> DFAS personnel used the 592 Balancing Desk Guide; however, a policy regarding document retention was not in place. Specifically, there was no requirement to retain the printed and reviewed report checklist, or the signed Report of Withholdings.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p><u>DFAS Cleveland:</u> 592 Reconciliations</p> <p>DFAS personnel used the 592 Balancing Desk Guide; however, a policy regarding document retention was not in place. Specifically, there was no requirement to retain the printed and reviewed report checklist or the signed Report of Withholdings.</p>
		<p>7.22 - Payroll transactions at the end of a payroll cycle are reconciled by supervisory personnel to ensure complete and consistent recording in the appropriate accounting period.</p>	<p>Inquired with appropriate personnel and inspected a random sample of 592 Reconciliations at the end of a payroll cycle to confirm they were reconciled in order to confirm complete and consistent recording in the appropriate accounting period.</p> <p>[All payroll offices]</p>	<p><u>DFAS Indianapolis:</u> DFAS was unable to provide 8 of 45 samples documenting final disbursement authorization.</p> <p><u>DFAS Cleveland:</u> 10 of 45 reconciliations were missing documentation of a final disbursement authorization.</p>
		<p>7.23 - Error reports, such as the Personnel Interface Invalid Report, and error warnings show rejected transactions with error messages that have clear, understandable corrective actions for each type of error.</p>	<p>Inquired with appropriate personnel and inspected a sample of Personnel Interface Invalid Reports to confirm the following:</p> <ul style="list-style-type: none"> <li>The reports show rejected transactions with error</li> </ul>	<p><u>DFAS Indianapolis:</u> DFAS was unable to provide 12 of 45 PIIRs.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		<p>Rejected data are automatically written to the Personnel Interface Invalid Report and held until corrected by payroll technicians. Each erroneous transaction is annotated with codes indicating the type of data error, date and time the transaction was processed and the error identified, and the identity of the user who originated the transaction.</p> <p>Users review the Personnel Interface Invalid Reports for data accuracy, validity, and completeness.</p> <p>A control group is responsible for controlling and monitoring rejected transactions included on the Personnel Interface Invalid Report.</p>	<p>messages that have clear, understandable corrective actions for each type of error.</p> <ul style="list-style-type: none"> <li>• The rejected data are automatically written on an automated error suspense file and held until corrected by payroll technicians. Each erroneous transaction is annotated with codes indicating the type of data error, date and time the transaction was processed, the error identified, and the identity of the user who originated the transaction.</li> <li>• Users review output for data accuracy, validity, and completeness.</li> <li>• The report is used for controlling and monitoring rejected transactions.</li> </ul> <p>[All payroll offices]</p>	<p>For the remaining 33 PIIRs:</p> <ul style="list-style-type: none"> <li>• 3 PIIRs did not include annotations using the proper standard codes.</li> <li>• 2 PIIRs did not include the dates the payroll technician addressed the errors.</li> </ul> <p><u>DFAS Cleveland:</u></p> <p>DFAS was unable to provide 16 of 45 PIIRs requested.</p> <p>Of the 29 PIIR reports provided:</p> <ul style="list-style-type: none"> <li>• 1 PIIR was missing the payroll technician's signature.</li> <li>• 1 PIIR did not include the dates the payroll technician addressed the errors.</li> </ul>
		<p>7.24 - Policies and procedures are documented to describe that capabilities exist for fiscal year-end, leave year-end, and calendar year-end processing and forfeitures in accordance with established</p>	<p>Inquired with appropriate personnel and inspected policies and procedures to confirm that capabilities exist for fiscal year-end, leave year-end, and calendar year-end processing and forfeitures in accordance with</p>	<p><u>DFAS Indianapolis:</u> <i>Management Summary Reports</i></p> <p>No policy was in place that</p>



No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		Government-wide and agency guidelines.	<p>established Government-wide and agency guidelines. Obtained and inspected Payroll Quality Review reports to confirm checklists are followed, and payroll steps have been performed.</p> <p>[All payroll offices]</p>	<p>required a complete and accurate listing of management summary reports generated and reviewed by Civilian Pay Processing Personnel.</p> <p>DFAS was unable to provide the Separation Actions without Separations Codes Desk Guide.</p> <p>The Less than \$1 Over \$5,000 Desk Guide did not have an increased threshold amount of \$10,000 in the review procedures.</p> <p><u>DFAS Cleveland:</u> <i>Management Summary Reports</i></p> <p>No policy was in place that required a complete and accurate listing of management summary reports generated and reviewed by Civilian Pay Processing personnel.</p> <p>DFAS was unable to provide the Desk Guides for the following critical reports:</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<ul style="list-style-type: none"> <li>• Separation Action without Separation Codes Desk Guide,</li> <li>• Dual SSN/Mongoose Desk Guide, and</li> <li>• P6702R01 - Invalid SSN/Deceased Employees/Negative Year-To-Date Desk Guide.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		7.25 - Payroll withholding table data is periodically reviewed by supervisory personnel for compliance with statutory requirements.	<p>Inspected a sample of payroll withholding table data updates to confirm that they are periodically updated by supervisory personnel for compliance with statutory requirements.</p> <p>[DFAS Saufley Field]</p>	No relevant exceptions noted.
		7.26 - The data processing control group has a schedule by application that shows when outputs should be completed, when they need to be distributed, who the recipients are, and the copies needed. The data processing control group reviews output products for general acceptability; and reconciles control information to determine completeness of processing.	<p>Inquired with appropriate personnel and inspected the schedules used by the data processing group to confirm that they:</p> <ul style="list-style-type: none"> <li>• had a schedule by application that shows when outputs need to be completed, when they need to be distributed, who the recipients are, and the copies needed;</li> <li>• reviewed output products for general acceptability; and</li> <li>• reconciled control information to determine completeness of processing.</li> </ul> <p>[DFAS Saufley Field]</p>	<p><u>DFAS Saufley Field:</u> DFAS was unable to provide operator jobs logs for 3 of the 18 randomly selected dates.</p>
		7.27 - Policies and procedures are documented to describe that current- or prior-period adjustments to employee's pay; including employee debt, tax deduction, or deductions not	Inquired with appropriate personnel and inspected policies and procedures to confirm that current- or prior-period adjustments to each employee's pay; including employee	<p><u>DFAS Indianapolis:</u> <i>Management Summary Reports</i></p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		<p>taken; are reported, reconciled, and approved.</p>	<p>debt, tax deduction, or deductions not taken; are reported, reconciled and approved.</p> <p>[All payroll offices]</p>	<p>No policy was in place that required a complete and accurate listing of management summary reports generated and reviewed by Civilian Pay Processing Personnel.</p> <p>DFAS was unable to provide the Separation Actions without Separations Codes Desk Guide.</p> <p>The Less than \$1 Over \$5,000 Desk Guide did not have an increased threshold amount of \$10,000 in the review procedures.</p> <p><u>DFAS Cleveland:</u></p> <p><i>Management Summary Reports</i></p> <p>No policy was in place that required a complete and accurate listing of management summary reports generated and reviewed by Civilian Pay Processing Personnel.</p> <p>DFAS was unable to provide the Desk Guides for the following critical</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				reports: <ul style="list-style-type: none"> <li>• Separation Action without Separation Codes Desk Guide,</li> <li>• Dual SSN/Mongoose Desk Guide, and</li> <li>• P6702R01 - Invalid SSN/Deceased Employees/Negative Year-To-Date Desk Guide.</li> </ul>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
8	<b>Data From Interfacing Systems</b>			
8	Controls provide reasonable assurance that data from interfacing systems are transferred timely and accurately.	8.1 - Policies and procedures are documented to describe that data transmissions between DCPS and user organizations are authorized, complete, accurate, and secure.	Inquired with appropriate personnel and inspected policies and procedures to confirm that data transmissions between DCPS and user organizations are authorized, complete, accurate, and secure.  [DFAS Saufley Field]	No relevant exceptions noted.
		8.2 - For interfacing systems, record counts are accumulated and compared to footer control totals to help determine the completeness of interface processing. Out-of-balance conditions are reported, corrected, and reentered.	Inquired with appropriate personnel and inspected interface files to confirm that record counts match control totals in the footer to determine completeness of interface processing and out-of-balance conditions are reported, corrected, and reentered.  [DFAS Saufley Field]	No relevant exceptions noted.
		8.3 - Batch transactions without pre-assigned serial numbers are automatically assigned a unique sequence number, which is used by the computer to monitor that all transactions are processed.	Inspected a batch transactions report to confirm that transactions without pre-assigned serial numbers are automatically assigned a unique sequence number.  [DFAS Saufley Field]	No relevant exceptions noted.

**General Computer Control Objectives, Control Activities, Tests Performed, and Results of Testing**

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
1	<b>Security Programs Effectiveness Monitoring</b>			
1.1	Controls provide reasonable assurance that the security program effectiveness is monitored and changes are made as needed.	<u>1.1.1 DISA DECC-MECH and DFAS Saufley Field</u> DoD and DFAS policy both direct that an annual Information Assurance (IA) review be performed.	<u>DISA DECC-MECH and DFAS Saufley Field</u> Inquired with the security officer to obtain an understanding of how management assessed the appropriateness of the security policies and compliance with them.	No relevant exceptions noted.
1.2	Management monitors compliance with policies and procedures.	<u>1.2.1 DISA DECC-MECH</u> The Director’s Policy Letters and SOP are reviewed and updated. Security Readiness Reviews (SRRs) are conducted at least every 3 years.	<u>DISA DECC-MECH</u> Inspected the DCPS Security Requirements and Information Systems Security Policy Certification Test and Evaluation Plan and Procedures to confirm that an annual IA review was conducted and that a comprehensive vulnerability management process was in place.	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
1.3	Corrective actions are effectively implemented.	<p><u>1.3.1 DISA DECC-MECH</u></p> <p>The Vulnerability Management System (VMS) 6.0 is used to track the status of outstanding Information Assurance Vulnerability Alerts (IAVAs) and the status of STIG findings from the SRR process. DISA DECC-MECH management is responsible for tracking and closing all IAVAs and STIG findings that resulted from the SRR process.</p> <p><u>1.3.2 DFAS Saufley Field</u></p> <p>Remediation plans detail corrective actions in response to findings identified in audits of DCPS or DFAS. Management has approved the remediation plan and monitors progress of the plan.</p>	<p><u>DISA DECC-MECH</u></p> <p>Inspected the SRR process to confirm that corrective actions are effectively implemented for identified SRR findings.</p> <p>Selected a sample of SRRs and inspected the VMS reports to confirm that findings identified by the SRR process have been addressed.</p> <p>Requested prior audit reports or reviews and confirmed that remediation had occurred for the findings and recommendations.</p> <p><u>DFAS Saufley Field</u></p> <p>Requested prior audit reports and confirmed that remediation has occurred for the findings and recommendations.</p> <p>Requested remediation plans intended to address previous findings to confirm that remediation had been initiated.</p>	<p><u>DISA DECC-MECH and DFAS Saufley Field:</u></p> <p>The prior year finding regarding payroll data transmitted through the NIPRNET unencrypted has not been resolved.</p>



No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
2	<b>Risk Assessment</b>			
2.1	Risk assessments are performed according to current Federal and DoD requirements.	<u>2.1.1 DISA DECC-MECH and DFAS Saufley Field</u> DoD and DFAS policy both direct that an annual IA review be conducted.	<u>DISA DECC-MECH</u> Inquired with the Information System Security Officer (ISSO) and related security personnel and inquired how often the risk assessment process occurs. Inspected the SRR process and confirmed how often it occurs and verified that deficiencies and corrective actions are tracked. Selected a sample of SRRs performed and inspected the VMS reports to confirm that findings identified by the SRR process have been addressed. <u>DFAS Saufley Field</u> Inquired with the ISSO and related security personnel and inquired how often the risk assessment process occurs. Inspected the last Risk Assessment, which should be included with the SSAA to confirm that risks are periodically assessed.	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
3	<b>Site Security Plans</b>			
3.1	Site security plans are documented, approved, and are current.	<u>3.1.1 DFAS Saufley Field</u> DoD and DFAS policy both direct that an annual IA review be conducted. Review appropriate generated documentation to ensure that these processes are accomplished.	<u>DFAS Saufley Field</u> Inspected the DCPS SSAA to confirm that it has been documented, kept current, and appropriately approved by management.  Inspected DCPS Systems Security Policy, Security Requirements, and Certification Test and Evaluation Plan and Procedures to confirm that each has been updated.	No relevant exceptions noted.
4	<b>Security Management Structure</b>			
4.1	A security management structure has been established with DCPS.	<u>4.1.1 DFAS Saufley Field</u> The DCPS SSAA describes the IA operations of the DoD information system and clearly delineates IA responsibilities and expected behavior of all personnel.	<u>DFAS Saufley Field</u> Confirmed through inquiry that a management structure had been established.  Obtained and inspected the security management organization chart.  Requested one position description for each function listed on the organization chart to confirm that positions were established in writing.  Inspected the SSAA for the security management structure. Confirmed that each position function is outlined in the SSAA.	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
4.2	Information security responsibilities are clearly assigned.	<p><u>4.2.1 DISA DECC-MECH and DFAS Saufley Field</u></p> <p>The DISA DECC-MECH SSAA and the DCPS SSAA both describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel.</p>	<p><u>DISA DECC-MECH</u></p> <p>Inspected signed rules of behavior statements for the DISA personnel with access to DCPS and the underlying operating system.</p> <p><u>DFAS Saufley Field</u></p> <p>Inspected the SSAA for security management responsibilities. Confirmed that each position outlined in the SSAA is filled by personnel and those personnel understand their duties.</p> <p>Inspected signed rules of behavior statements for DFAS personnel with access to DCPS.</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
4.3	Employees are aware of security policies.	<p><u>4.3.2 DFAS Saufley Field</u></p> <p>Ongoing security awareness programs are in place that include initial training and periodic refresher training.</p>	<p><u>DFAS Saufley Field</u></p> <p>Inspected the Security Awareness Training materials.</p> <p>Obtained a list of employees who have access to DCPS. Selected a sample of employees who have DCPS access and inspected their training files to confirm the completion of the necessary security training (and the required certifications) and that they are signed.</p> <p>Obtained evidence that management has active security awareness programs in place (for example, electronic mail files, or other policy distribution mechanisms) that proactively emphasize the security policies to data owners and users.</p>	The Information Assurance Manager and Information Assurance Officer (IAM/IAO) did not receive IAM/IAO certifications.
4.4	A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place.	<p><u>4.4.1 DISA DECC-MECH</u></p> <p>Vulnerabilities are tracked in the VMS database. Prior to connection to the network, the system administrator must generate a VC06 report detailing Information Assurance Vulnerability Management (IAVM) notices for the asset's operating system. All IAVM notices must be mitigated, and applicable patches must be loaded prior to connecting the asset to the network. Once all checklists have been applied from the STIG and the patches from the vulnerability alerts</p>	<p><u>DISA DECC-MECH</u></p> <p>Obtained the VMS reports for the audit period for DCPS and confirmed vulnerabilities are being tracked and resolved in a timely manner.</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		<p>have been installed, a self-assessment and a Retina network scan is conducted. Security assessments that require a scan use the Retina scanner and the FSO Full Scan Policy. The scan is conducted using a direct connection from the system running the scanner to the system being assessed or the site is authorized to connect the asset to an isolated network during the Retina scan. Each site then places their self-assessment in the VMS database. If the systems have a database, web server, or any other software that has a STIG, they must put those self-assessments in VMS as well. The network scan must be generated with all database instances and all web servers running.</p>		

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
5	<b>Personnel Policies</b>			
5.1	Employee (Government or contractor) background investigations, hiring, transferring, and termination policies address security and are in compliance with DoD Instruction 8500.2.	<u>DFAS Saufley Field</u> The DCPS SSAA requires system users to be subjected to various levels of Personnel Security Investigations based on the level of access or privileges they have within the systems. The higher the level of access, the more stringent the required investigation becomes. As a minimum, all DFAS DCPS personnel/employees (military, civilian, or contractors) will have a favorably completed the National Agency Check.	<u>DFAS Saufley Field</u> Requested, obtained, and inspected the policies and procedures for gaining access to sensitive information.  Obtained a listing of all personnel associated with DCPS. Selected a sample of DCPS users and obtained SAAR forms for each. Confirmed that each SAAR details the user's justification for access, security clearance level, and the proper approvals.	No relevant exceptions noted.
5.2	Job descriptions for Government employees have been documented, and employees understand their duties and responsibilities.	<u>5.2.1 DISA DECC-MECH and DFAS Saufley Field</u> Developed position descriptions for distinct system support positions.	<u>DISA DECC-MECH</u> Inspected the job descriptions for the applicable types of personnel.  <u>DFAS Saufley Field</u> Inspected the job descriptions for the applicable types of personnel listed in Control Objective # 5.1.	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		<p><u>5.2.2 DISA DECC-MECH and DFAS Saufley Field</u></p> <p>Position descriptions are available and performance plans are provided to assist employees in understanding their roles and responsibilities according to their assigned duties.</p>	<p><u>DISA DECC-MECH</u></p> <p>Selected a sample of employees and confirmed through inquiry that they understood their duties and responsibilities.</p> <p>Inspected documentation to confirm that employees have signed position descriptions.</p> <p><u>DFAS Saufley Field</u></p> <p>Selected a sample of employees and confirmed through inquiry that they understood their duties and responsibilities.</p> <p>Inspected documentation to confirm that employees have signed their performance plans.</p>	<p>No relevant exceptions noted.</p>
		<p><u>5.2.3 DFAS Saufley Field</u></p> <p>All DFAS personnel are required to complete initial and periodic IA training. This training helps the employee understand the importance of their roles and responsibilities.</p>	<p><u>DFAS Saufley Field</u></p> <p>Inspected the hiring, transfer, termination, and performance policies to confirm that they are documented and address security.</p> <p>Confirmed through inquiry that debriefs are conducted when employees are terminated and that a Human Resources Checklist is used to note the collection of DFAS property.</p> <p>Confirmed through inspection that an e-mail is sent to the system administrator to request that system access be removed for a terminated employee.</p>	<p>No relevant exceptions noted.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
5.3	Employee (Government or contractor) are adequately trained and possess the required skills.	<p><u>5.3.1 DISA DECC-MECH and DFAS Saufley Field</u></p> <p>A program is implemented to ensure that upon arrival (and periodically thereafter), all personnel receive training and familiarization to perform their assigned IA duties, to include familiarization with their prescribed roles in all IA-related plans, such as incident response, configuration management, and Continuity of Operations Plan (COOP) or disaster recovery.</p>	<p><u>DISA DECC-MECH</u></p> <p>Confirmed through inquiry that a training program has been established.</p> <p>Requested documentation to confirm the existence of this training program (for example, individual training plans, job-specific training plans, and policy for requirements of training).</p> <p>If training was conducted in-house, inspected the training materials to confirm that they provided personnel with adequate training and expertise.</p> <p>Selected a sample of employees who have access to DCPS and inspected their training records to confirm that specific job function training is occurring.</p> <p><u>DFAS Saufley Field</u></p> <p>Confirmed through inquiry that a training program has been established.</p> <p>Requested documentation to confirm the existence of this training program (for example, individual training plans, job-specific training plans, and policy for requirements of training).</p>	<p><u>DFAS Saufley Field:</u></p> <p>We noted that the IAM and IAO did not receive IAM/IAO certifications.</p>



No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			<p>If training was conducted in-house, inspected the training materials to confirm that they provided personnel with adequate training that is up to date.</p> <p>Selected a sample of employees who have access to DCPS and inspected their training records to confirm that job-specific training is occurring.</p>	

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
6	<b>Information Resource Classification</b>			
6.1	Resource classifications and related criteria have been established.	<p><u>6.1.1 DISA DECC-MECH</u></p> <p>DFAS management has classified DCPS according to appropriate MAC-level standards and identified DCPS in the Service-Level Agreement (SLA) between DISA and DFAS.</p> <p><u>DFAS Saufley Field</u></p> <p>DFAS management has classified DCPS according to appropriate MAC-level standards and identified DCPS in the SLA between DISA and DFAS.</p>	<p><u>DISA DECC-MECH</u></p> <p>Inquired with management as to the process for identifying and prioritizing critical data and operations.</p> <p>Obtained documentation that supports this process and confirmed that it is current and was approved by management.</p> <p><u>DFAS Saufley Field</u></p> <p>Inquired with management as to the process for identifying and prioritizing critical data and operations.</p> <p>Obtained documentation that supports this process and confirmed that it is current and was approved by management.</p>	No relevant exceptions noted.
		<p><u>6.1.2 DISA DECC-MECH</u></p> <p>DFAS management has identified DCPS resources supporting critical operations based on the nature and impact of the disaster. The resources are included in the DISA DECC-MECH Business Continuity Plan as prescribed in the SLA between DISA and DFAS.</p>	<p><u>DISA DECC-MECH</u></p> <p>Corroborated with key personnel that identification of resources supporting critical operations is based on the nature and impact of the disaster.</p> <p>Obtained and inspected the business continuity plan and confirmed that supporting critical operations are identified, and emergency priorities are</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		<p><u>DFAS Saufley Field</u></p> <p>DFAS management has identified DCPS resources supporting critical operations based on the nature and impact of the disaster. The resources are included in the DISA DECC-MECH Business Continuity Plan as prescribed in the SLA between DISA and DFAS.</p>	<p>established and approved by management.</p> <p><u>DFAS Saufley Field</u></p> <p>Corroborated with key personnel that identification of resources supporting critical operations is based on the nature and impact of the disaster.</p> <p>Obtained and inspected the business continuity plan and confirmed that supporting critical operations are identified, and emergency priorities are established and approved by management.</p>	
6.2	DFAS has classified all DFAS-owned assets according to criticality and sensitivity.	<p><u>6.2.1 DFAS Saufley Field</u></p> <p>Management has classified DCPS according to appropriate MAC-level standards.</p>	<p><u>DFAS Saufley Field</u></p> <p>Inspected the DCPS SSAA and confirmed that a MAC level had been assigned to DCPS.</p> <p>Inquired with data owners and confirmed that a MAC level has been assigned to DCPS.</p> <p>Inspected the DCPS SLA between DFAS and DISA to determine the classification of DCPS communicated to DISA.</p>	No relevant exceptions noted.
6.3	Data management and the disposition and sharing of data requirements are identified in the SLAs.	<p><u>6.3.1 DFAS Saufley Field</u></p> <p>Documented policies and procedures are in the DCPS SSAA that governs the sharing of data.</p>	<p><u>DFAS Saufley Field</u></p> <p>Inspected documents authorizing file sharing and file sharing agreements and confirmed that the owners approve the</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			<p>sharing of data. In many cases, these documents are called a Memorandum of Understanding or SLA.</p> <p>Inspected the DCPS SSAA and confirmed that a MAC level had been assigned to DCPS.</p> <p>Inquired with data owners and confirmed that a MAC level has been assigned to DCPS.</p> <p>Inquired with data owners and confirmed that a Memorandum of Understanding has been developed and is in place for each DCPS interface.</p>	
6.4	DCPS has logical controls over data files and software programs.	<p><u>6.4.1 DFAS Saufley Field</u></p> <p>The SAAR is used to identify authorized users and control their access.</p>	<p><u>DFAS Saufley Field</u></p> <p>Requested a complete DCPS user list. Selected a random sample of users from the list and inspected their user access request forms for existence and approval by management.</p> <p>Inspected the application to confirm that users must have possessed a valid User ID and password to gain access to the system.</p> <p>Interviewed owners and inspected supporting documentation to confirm that inappropriate access is removed in a timely manner.</p> <p>Interviewed security managers and confirmed that supporting documentation</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			<p>was provided to them.</p> <p>Obtained a representative sample of profile changes and activity logs and confirmed that management reviewed the changes and logs.</p> <p>Obtained a list of recently terminated employees from the personnel office. Selected a random sample of terminated employees and confirmed that system access was promptly terminated.</p>	
		<p><u>6.4.2 DISA DECC-MECH</u></p> <p>The DISA System Support Office, a unit independent of DISA DECC-MECH operations, is responsible for maintaining the system libraries; however, DISA DECC-MECH performs the library installation. Access to system libraries is restricted to authorized individuals, including system programmers at the DISA System Support Office and DISA DECC-MECH.</p>	<p><u>DISA DECC-MECH</u></p> <p>Confirmed through inquiry and inspection of the root access users for the DCPS servers that access restrictions have been established around the data files and software programs.</p> <p>Inspected the access logs and corroborated with management that the access logs are reviewed for inappropriate access and that system libraries are managed and maintained to protect privileged programs.</p>	<p>No relevant exceptions noted.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
7	<b>User Account Management</b>			
7.1	<p>Authorized users and their access rights are identified for DISA-/DFAS-owned assets.</p> <p>Access authorizations are appropriately limited.</p>	<p><u>7.1.1 DISA DECC-MECH and DFAS Saufley Field</u></p> <p>User accounts are suspended after 35 days of no activity (60 days for TSO and payroll offices) and removed after 180 days of no activity. Accounts are approved by IA officers.</p>	<p><u>DISA DECC-MECH</u></p> <p>Inspected the policies and procedures for restricting access to the systems software to confirm that they were up-to-date.</p> <p>Generated a list from the Discretionary Access Control database of individuals who had direct access to the system software and selected a random sample of users with direct access.</p> <p>For each user selected, confirmed with key management personnel that these users were authorized to have this access.</p> <p>Inquired with key management that suspension and termination of access is performed according to the policies and procedures.</p> <p>Interviewed owners and inspected supporting documentation to confirm that inappropriate access is removed in a timely manner.</p> <p>Obtained a list of recently terminated employees from the personnel office. Selected a random sample of terminated employees and confirmed that system access was promptly terminated.</p> <p><u>DFAS Saufley Field</u></p> <p>Inspected the policies and procedures for</p>	<p>No relevant exceptions noted.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			<p>restricting access to the DCPS application software to confirm that they were up-to-date.</p> <p>Generated a list from the Discretionary Access Control database of individuals who had direct access to the DCPS application software and selected a random sample of users with direct access. For each user selected, confirmed with key management personnel that these users were authorized to have this access.</p> <p>Inquired with key management that suspension and termination of access is performed according to the policies and procedures.</p> <p>Interviewed owners and inspected supporting documentation to confirm that inappropriate access is removed in a timely manner.</p> <p>Obtained a list of recently terminated employees from personnel office. Selected a random sample of terminated employees and confirmed that system access was promptly terminated.</p>	
7.2	<p>IAOs or SAs periodically review authorization listings to determine appropriateness.</p> <p>Policies and techniques have been implemented for</p>	<p><u>7.2.1 DISA DECC-MECH</u></p> <p>Access to the system software is administered based on roles.</p>	<p><u>DISA DECC-MECH</u></p> <p>Inquired with key personnel to determine how root and/or privileged access is administered.</p> <p>Obtained the list of individuals with root and or privileged access.</p>	<p>No relevant exceptions noted.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
	using and monitoring the use of system utilities.		<p>Inquired with management if root and privileged access is appropriate and that the use of these accounts is logged.</p> <p>Inspected a random sample of the audit logs from the DCPS servers to confirm that personnel review the logs on a regular basis and that any issues noted are documented and researched.</p>	
7.3	Emergency and temporary access is controlled.	<p><u>7.3.1 DISA DECC-MECH and DFAS Saufley Field</u></p> <p>Emergency and temporary access authorization is controlled in accordance with DoD 5200.1-R, DoD 5200.2-R, DoDD 8500.1, and DoDI 8500.2. Accounts are approved by the IA officers.</p>	<p><u>DISA DECC-MECH</u></p> <p>Inspected the emergency and temporary access policy.</p> <p>Selected a random sample of emergency and temporary access and confirmed that:</p> <ul style="list-style-type: none"> <li>• the authorization was approved and that the access was closed in a timely manner,</li> <li>• the emergency and temporary access list is periodically reviewed, and</li> <li>• temporary access authorizations were established for least privileged, need-to-know access.</li> </ul> <p><u>DFAS Saufley Field</u></p> <p>Inspected the emergency and temporary access policy.</p> <p>Selected a random sample of emergency and temporary access and confirmed that:</p>	No relevant exceptions noted.



No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			<ul style="list-style-type: none"> <li>• the authorization was approved and that the access was closed in a timely manner,</li> <li>• the emergency and temporary access list is periodically reviewed, and</li> <li>• temporary access authorizations were established for least privileged, need-to-know access.</li> </ul>	
7.4	Group authenticators for application or network access may be used only in conjunction with an individual authenticator	<u>7.4.1 DFAS Saufley Field</u> Group authenticators are not used for DCPS or network access. Upon initial system login, a user's actions are tracked based on their unique user account.	<u>DFAS Saufley Field</u> Confirmed through inquiry that group authenticators for the application and network are used. Inquired why group authenticators are used. Inquired if users are authenticated individually prior to the use of a group authenticator. Confirmed through observation that group authentication is used by the operations group; however, confirmed that operator job logs are used to record the actions of the operators, which use the group authentication.	DFAS was unable to provide 3 of 18 randomly selected dates for operator job logs requested.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
8	<b>Physical Security</b>			
8.2	Building, administration, and computer facility physical controls have been implemented.	<p><u>DFAS Saufley Field</u></p> <p>DFAS facilities at DFAS Saufley Field have implemented adequate physical security controls in accordance with DODI 8500.2.</p> <p>Physical access points are guarded or alarmed 24 hours a day.</p> <p>The Random Anti-Terrorism Measures process is in place and it includes periodic, unannounced attempts to penetrate DFAS facilities. Only authorized personnel with appropriate access approval are granted physical access.</p>	<p><u>DFAS Saufley Field</u></p> <p>Inquired with facility management as to the physical security controls in place. Confirmed through observation that these controls are in place. Obtained results of the most recent facility penetration testing and confirmed that management reviewed the results of the test.</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
8.3	Visitors are controlled.	<p><u>8.3.2 DFAS Saufley Field</u></p> <p>All visitors must sign in and out on the Visitor Control Log located in the main lobby.</p> <p>The DCPS SSAA requires all non-cleared personnel to be escorted at all times while inside the building.</p>	<p><u>DFAS Saufley Field</u></p> <p>Inspected the visitor policies and procedures to confirm they are documented.</p> <p>Confirmed through inquiry that all visitors are controlled.</p> <p>Confirmed through inquiry and observation that visitor access to DoD information was determined by both its classification and user need-to-know.</p> <p>Obtained the visitor check-in log for a random sample of normal business days. Confirmed that the log has been completed according to the visitor policies and procedures.</p>	<p>The Administrator 6H visitor policy did not include policies and procedures for granting access to visitors for an extended length of time.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
9	<b>Logical Access</b>			
9.1	Access settings have been implemented in accordance with the access authorizations established by the resource owners.	<p><u>9.1.1 DISA DECC-MECH</u></p> <p>Access settings have been implemented in accordance with the access authorizations established by signature authority of the resource owner listed on the SAAR and in accordance with DoDD 8500.1, DoDI 8500.2, and STIGs.</p> <p><u>9.1.2 DFAS Saufley Field</u></p> <p>The TSO assigns security profiles to each user ID based on need-to-know as demonstrated by an approved SAAR for system access. The DFAS Saufley Field database administrator also assigns security profiles to development users through the Integrated Database Management System (IDMS), which restricts access to program libraries and databases.</p>	<p><u>DISA DECC-MECH</u></p> <p>Obtained a random sample of users with access to DCPS Logical Partition (LPAR) and obtained the SAAR for the sampled personnel. Confirmed that each SAAR details the user's justification for access and security clearance level, and that each SAAR is properly approved.</p> <p><u>DFAS Saufley Field</u></p> <p>Observed the DCPS system to confirm that each user account was assigned a security profile that restricts access by module or program.</p> <p>Requested a complete DCPS user list. Selected a random sample of users from the list and inspected the SAARs for the user's justification for access, security clearance level, and approval by management.</p>	No relevant exceptions noted.
9.2	Passwords, tokens, or other devices are used to identify and authenticate users.	<p><u>9.2.1 DFAS Saufley Field</u></p> <p>User IDs and passwords are configured according to DoD standards.</p>	<p><u>DFAS Saufley Field</u></p> <p>Observed that each user account was assigned a security profile that restricted access by module and program.</p> <p>Inspected the DCPS application to confirm that users needed a valid user ID and password to gain access to the system.</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			Inspected system parameters to verify that the system requires a user ID and password.	
		<p><u>9.2.2 DISA DECC-MECH</u></p> <p>Multiple layers of access controls are used including, a Common Access Card and personal identification number; a DCPS user ID and password; and a RSA SecurID for database administration, configuration management, security, and tech support.</p>	<p><u>DISA DECC-MECH</u></p> <p>Confirmed through inquiry and observation that passwords are used to authenticate users.</p> <p>Inspected system parameters to verify that the system requires a user ID and password.</p> <p>Inspected the SSAA to confirm that authentication devices are in compliance with DoD standards.</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
<b>10</b>	<b>Network and Telecommunications</b>			
<b>10.1</b>	<p>Telecommunication defense capabilities are implemented.</p> <p>Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography.</p>	<p><u>10.1.1 DISA DECC Montgomery</u></p> <p>DISA DECC-MECH is in the process of encrypting all data streams to the Federal Information Processing Standards 140-2, "Security Requirements for Cryptographic Modules."</p>	<p><u>DISA DECC Montgomery</u></p> <p>Inquired with security personnel if DCPS data are transmitted through a commercial or wireless network. Inquired with security personnel to determine whether NIST cryptography was used to protect information transmitted over commercial or wireless networks.</p>	<p>We noted payroll data transmitted through the NIPRNET are unencrypted.</p>
<b>10.2</b>	<p>Network defense capabilities are implemented. At a minimum, medium-robustness Commercial Off-the-Shelf (COTS) IA and IA-enabled products are used to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system.</p>	<p><u>10.2.1 DISA DECC Montgomery</u></p> <p>Appropriate IA products are implemented to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system.</p> <p>Telnet access to the DCPS mainframe domain is secured using Secure Web Access (SWA). All DCPS users must use SWA when accessing DCPS.</p>	<p><u>DISA DECC Montgomery</u></p> <p>Inspected the DISA SAS 70 Report to identify any issues as a result of the testing.</p> <p>Inquired with system administrators to determine whether telnet access to the DCPS mainframe domain is secured using SWA.</p>	<p>The IA-enabled products, including routers and firewalls, are not configured to "deny by default," and DISA DECC-MECH firewalls are not STIG compliant.</p>
<b>10.3</b>	<p>Remote and dial-up capabilities are controlled.</p>	<p><u>10.3.1 DISA DECC Montgomery</u></p> <p>Remote access to the Internet is regulated by positive technical controls, such as proxy services and</p>	<p><u>DISA DECC Montgomery</u></p> <p>Inspected the DISA SAS 70 Report to identify any issues as a result of the testing.</p>	<p>Noted users did not use DoD-issued computers for remote telnet access</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		<p>screened subnets, also called demilitarized zones (DMZ), or through systems that are isolated from all other DoD information systems through physical means.</p> <p>There is a remote dial-in router provided for systems administrators that requires Secure Shell restrictions. The Exchange System Manager is installed on some of these systems.</p> <p>System administrators must use the DISA CSD out-of-band network to access all servers for which they are responsible for the administration and maintenance.</p> <p>There is a “deny-by-default” policy implemented at DISA DECC-MECH that prohibits data traffic over ports and protocols unless specifically allowed in the ACL rules.</p>		<p>through the MIAP application to the MZF LPAR.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
10.4	Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures is planned, scheduled, and conducted.	<u>10.4.1 DISA DECC-MECH</u> DISA DECC-MECH performs monthly scans to check for any DCPS network vulnerabilities. The DCPS system and hardware are reviewed through periodic SRR reviews that are conducted by FSO on the DCPS mainframe domain.	<u>DISA DECC-MECH</u> Confirmed through inquiry that conformance testing was performed that included periodic, unannounced, in-depth monitoring and provided for specific penetration testing to confirm compliance with vulnerability mitigation procedures.  Obtained and inspected documentation produced from this conformance testing to confirm that vulnerability scans were completed.	No relevant exceptions noted.
11	[This control objective was intentionally left blank.]			



No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
12	<b>Access Monitoring</b>			
12.1	Audit trails are maintained.	<p><u>12.1.1 DISA DECC-MECH and DFAS Saufley Field</u></p> <p>A security audit trail is implemented for each system that documents the identity of each person/device having access to a system, the time of that access, user activity, and any actions that, attempt to change security levels or privileges established for the user. The audit trail is maintained by DISA.</p>	<p><u>DISA DECC-MECH</u></p> <p>Confirmed through inquiry that audit trails are implemented for the MZF LPAR.</p> <p>Inspected the audit trails available and determined what information is being logged.</p> <p>Confirmed through inquiry and inspection that audit trails are maintained for at least 5 years.</p> <p>Confirmed through inquiry and inspection that the log is reviewed and signed by management.</p> <p><u>DFAS Saufley Field</u></p> <p>Confirmed through inquiry that audit trails are implemented for the application.</p> <p>Inspected the audit trails available and determined what information is being logged.</p> <p>Confirmed through inquiry and inspection that audit trails are maintained for at least 5 years.</p> <p>Confirmed through inquiry and inspection that the log is reviewed and signed by management.</p>	<p><u>DISA DECC-MECH</u></p> <p>No relevant exceptions noted.</p> <p><u>DFAS Saufley Field:</u></p> <p>DFAS was unable to provide 3 of 54 audit logs.</p> <p>Of 54 audit logs, 10 lacked evidence of management review.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		<p><u>12.1.3 DFAS Saufley Field</u></p> <p>Adheres to DITSCAP requirements for system access and content, retention, and protection of audit trails. The most recent testing of compliance with DITSCAP guidance is contained in the DCPS SSAA, Appendices H and P.</p>	<p><u>DFAS Saufley Field</u></p> <p>Inspected the policy for protecting the audit trails and confirmed that the policy limits access to audit trails.</p> <p>Confirmed through inquiry and inspection that audit logs included activities that might modify, bypass, or negate safeguards controlled by the system so that the audit trails should be protected against unauthorized access, modification, or deletion.</p> <p>Observed that only select/limited number of individuals, such as the ISSO and Information Assurance Manager, have access to the audit trails.</p>	<p>No relevant exceptions noted.</p>
<p><b>12.4</b></p>	<p>Suspicious network access activity is investigated and appropriate action is taken.</p> <p>Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within DoD information systems.</p>	<p><u>12.4.2 DFAS Saufley Field</u></p> <p>Desktop Management Interface controls the configuration of computers, and instant messaging programs are not authorized. Saufley Field monitors application usage through an automated software auditing application that runs regularly when users logon to their workstation.</p> <p>Instant messaging programs are identified as part of that auditing process.</p>	<p><u>DFAS Saufley Field</u></p> <p>Confirmed through inquiry with key personnel that the use of instant messaging is against DoD policy. Inquired to determine how instant messaging is controlled. Inspected firewall rules to confirm that instant messaging is blocked.</p>	<p>No relevant exceptions noted.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
13	<b>DCPS Change Management</b>			
13.1	DISA or DFAS-initiated application, software, or hardware modifications are authorized, and the documentation is maintained.	<p><u>13.1.1 DISA DECC-MECH</u></p> <p>Procedures addressing the testing of patches, upgrades, and new Automated Information System applications are documented.</p> <p>All changes to information systems at DISA DECC-MECH are brought before at least one of two Change Control Boards (CCBs). DISA headquarters has an Executive Software CCB (ESCCB) that is responsible for reviewing all major system changes, including new versions, new software, and the removal of software. There is also a local CCB at DISA DECC-MECH that meets on a weekly basis. The local CCB is responsible for reviewing all operating system upgrades and fixes. The local CCB is also responsible for alerting the customer to the change, obtaining the customer approval before proceeding, and maintaining the change control records.</p> <p><u>13.1.2 DISA DECC-MECH</u></p> <p>The DISA Executive Software CCB consists of representative of DISA management, as well as all the DISA</p>	<p><u>DISA DECC-MECH</u></p> <p>Obtained and inspected the change management policies and procedures for systems software to confirm that they exist and are current.</p> <p>Requested the full population of code/database modifications from the DCPS production code library which occurred during the audit period under review (10/01/07 through 3/31/08) and traced a sample of modifications to an approved System Change Request (SCR).</p> <p>For the modifications selected, obtained the change request document and confirmed that it was approved by key personnel prior to implementation.</p> <p>Confirmed that each modification was tested and the test results were approved prior to the modification being implemented.</p> <p>Confirmed the modification is documented by inspecting the SCR; System Test Plan; detailed system specifications; and unit, system, and acceptance testing results.</p>	We could not confirm that changes were tested prior to implementation due to the lack of traceability between the MZO change request tickets and the MZF change tickets.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		<p>DECCs. The DISA DECC-MECH local CCB consists of all department heads and the Information Assurance Manager.</p>		
		<p><u>13.1.3 DFAS Saufley Field</u></p> <p>Testing of changes follows the approved process outlined in the DFAS TSO Business Process Handbook prior to implementation.</p> <p>A Testing Deficiency Report is issued for SCRs with negative test results, and the Transportation Discrepancy Report is routed to the appropriate individuals. If necessary, an amendment is issued and it processes through the same approval process as an SCR.</p>	<p><u>DFAS Saufley Field</u></p> <p>Using the same random sample selected for control objective 13.1, we confirmed that the DCPS application changes followed the appropriate test and migration process by inspecting the following for completeness, authorization, and software quality requirements:</p> <ul style="list-style-type: none"> <li>• system test plan;</li> <li>• detailed system specifications; and</li> <li>• unit, system, and acceptance testing results.</li> </ul> <p>Inquired with DCPS security personnel as to his/her roles and responsibilities for the release of security-related changes included in DCPS releases.</p> <p>Inspected release notes for the major DCPS production releases that occurred during the audit period.</p>	<p>No relevant exceptions noted.</p>
		<p><u>13.1.4 DFAS Saufley Field</u></p> <p>Release management staff is responsible for ensuring that all</p>	<p><u>DFAS Saufley Field</u></p> <p>Using the same random sample selected for control objective 13.1, confirmed that</p>	<p>No relevant exceptions noted.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		programs are labeled and inventoried within the appropriate library.	the changes had been labeled, assigned an ID, and inventoried.	
13.2	New and modified application, hardware, and operating system or utility software is tested and controlled according to specific criteria.	<u>13.2.1 DFAS Saufley Field</u> Release management staff is responsible for distribution or implementation of new or revised software.	<u>DFAS Saufley Field</u> Using the same random sample selected for control objective 13.1, confirmed that the change followed the appropriate distribution process by inspecting the Release Authorization Report for completeness and authorization.	No documentation exists that states which configurable items are required to be tested before implementation. However, we noted that the Business Process Handbook is under revision to include the testable types of configurable items.
13.3	Emergency changes are promptly approved.	<u>13.3.1 DFAS Saufley Field</u> A Configuration Management Plan is implemented for software modifications. All modifications must go through the SCR process and receive proper approval prior to implementation, including emergency changes made during business hours. Emergency changes that arise during non-business hours may be implemented prior to SCR approval; however, the SCRs are approved through the change process the next day.	<u>DFAS Saufley Field</u> Using the same random sample selected for control objective 13.1, we confirmed through inspection that the DCPS emergency changes have been authorized by the program manager and/or software director and traced each SCR identified in the Release Authorization Report to confirm it has been approved by the software director.	No relevant exceptions noted.
13.4	Movement of programs and data among libraries is controlled.	<u>13.4.1 DFAS Saufley Field</u> The system administrator manages access rights to the program libraries	<u>DFAS Saufley Field</u> Observed the DCPS librarian to determine how the development and	We were unable to confirm that two of the five DCPS users

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		and databases through ACF2. The database administrator grants access to the appropriate development/production environments through IDMS. IDMS controls versioning in both the development and production environments.	production libraries are controlled. Inspected the access control lists for the production and development libraries (directories) to confirm that only authorized personnel have access.	obtained authorization to access both the MZO development LPAR and MZF production LPAR.
13.5	Use of public domain and personal software is restricted.	<u>13.5.1 DFAS Saufley Field</u> DFAS workstations and LANs do not allow any use of public domain and/or personal software. DCPS is on the mainframe and all utilities needed are on the mainframe (which is DISA-driven).	<u>DFAS Saufley Field</u> Inspected the DCPS SSAA to confirm that personal software is restricted. Inspected a listing of approved software to confirm such a list exists.	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
13.6	Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.	<p><u>13.6.1 DISA DECC-MECH</u></p> <p>All changes are captured in the Change Management System (Change Management 2000). Information included in each change record is the requested time and date of implementation, the action to occur, and justification for the action. The change is then presented to the local CCB where the change is assessed for IA and accreditation impact. The change is only implemented after approval from the CCB and testing is completed and reviewed.</p> <p><u>13.6.2 DFAS Saufley Field</u></p> <p>All changes are captured in the Change Management Information System. Information included in each change record is the implementation, the action to occur, and justification for the action. In addition, all changes are assessed by the IA officers.</p>	<p><u>DISA DECC-MECH</u></p> <p>Obtained the CCB meeting minutes for that random sample of changes previously noted. Confirmed the CCB meeting minutes included the discussion of the DCPS changes and confirmed whether management assessed the change for IA and accreditation impact.</p> <p>Determined whether the changes were approved by the CCB and testing has been completed and approved prior to implementation into the production environment.</p> <p><u>DFAS Saufley Field</u></p> <p>Using the same random sample selected for control objective 13.1, confirmed that the change record includes the requested time and date of implementation, the action to occur, and justification for the action.</p>	<p><u>DISA DECC-MECH:</u></p> <p>We could not confirm that changes were tested prior to implementation due to the lack of traceability between the MZO change request tickets and the MZF change tickets.</p> <p><u>DFAS Saufley Field:</u></p> <p>No relevant exceptions noted.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
14	<b>Data Retention</b>			
14.1	Data and program back-up procedures have been implemented.	<p><u>14.1.1 DFAS Saufley Field</u></p> <p>Data and program back-up procedures have been established by DFAS management</p> <p><u>DISA DECC-MECH</u></p> <p>Data and program back-up procedures have been established by DFAS management and are included in the DISA DECC-MECH Business Continuity Plan as prescribed in the SLA between DISA and DFAS.</p>	<p><u>DFAS Saufley Field</u></p> <p>Obtained the Business Continuity Plan to confirm that it specifies the data and program back-up procedures that have been implemented related to DCPS.</p> <p>Inquired with key personnel that resources are dedicated to the periodic backing-up and restoration of data stored on network share drives.</p> <p><u>DISA DECC-MECH</u></p> <p>Obtained the Business Continuity Plan to confirm that it specifies the data and program back-up procedures that have been implemented related to DCPS.</p> <p>Inquired with key personnel that resources are dedicated to the periodic backing-up and restoration of data stored on network share drives.</p> <p>Confirmed how often backups are performed, shipped to an offsite facility, and that the backups are maintained at the offsite facility in a fire rated container.</p> <p>Selected a random sample of dates, which occurred during the audit period, and obtained the back-up logs. Confirmed through inspection that the log is completed, based on the back-up policies and procedures.</p>	<p><u>DFAS Saufley Field:</u></p> <p>No relevant exceptions noted.</p> <p><u>DISA DECC-MECH:</u></p> <p>The Tape Library Procedures did not include an update to reflect the new process and storage facility used for back-up tapes.</p>



---

**Section IV: Supplemental Information Provided  
by the Defense Finance and Accounting Service and the  
Defense Information Systems Agency**

---



## **IV. Supplemental Information Provided by the Defense Finance and Accounting Service and the Defense Information Systems Agency**

### **Introduction**

DFAS and DISA have prepared this section and it is included to provide user organizations with information DFAS and DISA believes will be of interest to such organizations. However, this information is not covered within the scope or control objectives established for the SAS 70 review. Specifically, this section includes a summary of procedures that DFAS and DISA have implemented to enable them to recover from a disaster affecting a Payroll Office, the TSOPE, or DISA DECC-MECH.

This information has not been subjected to the procedures applied to the audit of the description of controls presented in Sections II and III of this report. As a result, the DoD OIG expresses no opinion regarding the completeness and accuracy of this information.

### **TSOPE Specific Business Continuity Plans**

The DCPS production support Continuity of Operations Plan (COOP) provides an action plan to be implemented when a disaster or impending threat would render DCPS production support inoperable (for example, hurricane, damage to TSOPE facilities due to fire). This plan is evaluated and updated on an annual basis and is implemented locally at each of the established DCPS Payroll Offices. If an impending threat or event occurs, production support control for DCPS is transferred to an alternate-processing site. Currently, that site is DFAS Indianapolis, Indiana. The COOP includes the names of DCPS staff members who will serve as a pool of resources to be mobilized to execute the plan and a list of documentation and supplies that are necessary to support the mobilized team.

Team members are comprised of DCPS development staff members across many divisions and branches. TSOPE designates two members of the management team to be responsible for COOP execution. One is mobilized with the team and is responsible for team activities and communication with TSOPE while deployed to the COOP recovery site. The other serves as the team's liaison at TSOPE and is responsible for relaying current operational status, current area weather conditions, and other pertinent information to the mobilized team. The team is further divided into two teams, with each covering a 12-hour shift. Team leaders are appointed for the respective shift teams. The DCPS project management staff coordinate and are involved in each step included in planning and executing the COOP. Although this plan works for any type of disaster where production support becomes inoperable, it has been executed several times in the past few years during impending disastrous weather conditions, such as hurricanes.

## **DECC-MECH Business Continuity Plans**

To accommodate a major disaster at any major DISA processing center, DISA has established an Enterprise Business Continuity Program. The DISA plan uses multiple internal locations and, for mainframe processing, utilizes the Assured Computing Environment infrastructure elements located at DISA DECC-MECH and Ogden. DISA DECC-MECH and Ogden is equipped with computational direct access storage devices and telecommunication resources necessary to provide a fully functional host site with the capacity to support a major disaster at any DISA center with mainframe processing.

The COOP support agreement between DFAS, as the customer, and DISA, as the provider of processing systems and communications services, describes a process for restoring host-site processing in the event of a major disaster. The plan also addresses the timely resolution of problems during other disruptions that adversely affect DCPS processing. The plan, as it relates to DCPS, details data restoration procedures for the MZF z/OS operating system, the DCPS Integrated Database Management System, and related mid-tier servers and communication devices. Replicated data and back-up tapes containing incremental daily and complete weekly backups are rotated offsite to designated locations, on a predetermined schedule, for storage.

The Crisis Management Team at DISA DECC-MECH is responsible for declaring that a disaster has occurred and activating the Business Continuity Plan. Once a disaster has been declared, the Crisis Management Team activates the following response teams: Communications Team, Recovery Coordination Team, Site Recovery Team, and the Crisis Support Team. Each team has a specific set of responsibilities defined in the Business Continuity Plan. The contact information for each individual on each team is also included in the Business Continuity Plan. The plan is required to be tested on an annual basis. The Business Continuity Plan was tested in November 2005. TSOPE personnel participate in the yearly COOP exercise to ensure that the process works correctly and documentation is updated appropriately.

## **DFAS Indianapolis 592 Reconciliation Report Policies and Procedures**

Policies and procedures for performing the 592 Payroll for Personal Services Payroll Certification and Summary Report reconciliation has been developed and documented at the DFAS Indianapolis Payroll Office. Uniform procedures are in place for both DFAS Civilian Payroll Offices for reconciliation of the 592.

## **DCPS Password Configuration**

The access control software for the environment on which DCPS resides, ACF2 supports complex passwords and complex passwords are utilized.

# Acronyms and Abbreviations

ACF2	Access Control Facility 2
ATO	Authority to Operate
BBG	Broadcast Board of Governors
BRAC	Base Realignment and Closure
CCB	Change Control Board
COOP	Continuity of Operations Plan
CSR	Customer Service Representative
DAA	Designated Approval Authority
DCPS	Defense Civilian Pay System
DECC	Defense Enterprise Computing Center
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DoE	Department of Energy
EOP	Executive Office of the President
EPA	Environmental Protection Agency
FSO	Field Security Operations
HHS	Health and Human Services
IA	Information Assurance
IDMS	Integrated Database Management System
IS	Information Security
ISSO	Information System Security Officer
LAN	Local Area Network
LPAR	Logical Partition
MAC	Mission Assurance Category
MECH	Mechanicsburg
MIAP	Multi-Host Internet Access Portal
NIPRNET	Non-Classified Internet Protocol Router Network
NSA	National Security Agency
OIG	Office of the Inspector General
OLQ	Online Queries
PIIR	Personnel Interface Invalid Report
SAAR	Systems Access Authorization Request
SAS 70	Standards of Auditing Standards 70
SCR	System Change Request
SLA	Service-Level Agreement
SMC	System Management Center

SOP	Standard Operating Procedure
SRR	System Readiness Review
SSAA	System Security Authorization Agreement
SSN	Social Security Number
STIG	Security Technical Implementation Guide
SWA	Secure Web Access
TASO	Terminal Area Security Officer
TSO	Technology Services Organization
TSOPE	Technology Services Engineering Organization in Pensacola
TSP	Thrift Savings Plan
VA	Veterans Affairs
VMS	Vulnerability Management System
VPN	Virtual Private Network

## **Team Members**

The Defense Financial Auditing Service, DoD OIG, in conjunction with contract auditors produced this report. Personnel from the Technical Assessment Directorate and Quantitative Methods Directorate, DoD OIG, also contributed to the report.

Patricia A. Marsh  
Patricia Remington  
Kenneth H. Stavenjord  
Donna A. Roberts  
Mihn Tran  
Ahn Tran  
Ann Thompson  
Carl L. Adams  
Anissa M. Nash  
Kiana E. Silver  
Shawn Sparks  
Brian Royer  
Alberto Calimano-Colon



# Inspector General Department of Defense

