

---

September 28, 2006

---



# Information Technology Management

Report on Defense Civilian Pay  
System Controls Placed in Operation  
and Tests of Operating Effectiveness  
for the Period July 1, 2005, through  
June 30, 2006  
(D-2006-120)

---

Department of Defense  
Office of Inspector General

---

*Quality*

*Integrity*

*Accountability*

### **Additional Information and Copies**

The Department of Defense Office of the Deputy Inspector General for Auditing, Defense Financial Auditing Service prepared this report. If you have questions or would like to obtain additional copies of the draft report, contact Mr. Michael Perkins at (703) 325-3557 (DSN 221-3557) or Mr. Sean Keaney at (703) 428-1448 (DSN 328-1448).

### **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) 604-8940 (DSN 664-8940) 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.osd.mil](mailto:hotline@dodig.osd.mil) [www.dodig.mil/hotline](http://www.dodig.mil/hotline)



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

September 28, 2006

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 July 1, 2005, through  
June 30, 2006 (Report No. D-2006-120)

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 Mr. Michael Perkins at (703) 325-3557 (DSN 221-3557) or Sean J. Keaney at  
(703) 428-1448 (DSN 328-1448). The audit team members are listed inside the back  
cover.

By direction of the Deputy Inspector General for Auditing:

*Patricia A. Marsh*  
for Paul J. Granetto, 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 DCPS Operations and Controls Provided by DFAS and DISA	11
<b>Section III</b>	
Control Objectives, Control Activities, and Tests of Operating Effectiveness	23
<b>Section IV</b>	
Supplemental Information Provided by DFAS and DISA	89
<b>Acronyms and Abbreviations</b>	93
<b>Report Distribution</b>	94

## FOREWORD

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

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, the Environmental Protection Agency, and the Executive Office of the President. In 2005, DCPS processed approximately \$42.3 billion in pay transactions and paid approximately 789,000 employees on a biweekly basis.

The DoD Office of Inspector General 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 agencies prepare and conduct audits of financial statements. The reliability of information in DCPS directly impacts the Defense Department's ability to provide reliable, and ultimately auditable, financial statements, which is key to achieving the goals of the Chief Financial Officers Act.

This audit assessed DCPS application and general computer controls and related processing. DFAS and DISA are responsible for managing and maintaining DCPS application and general computer controls. This report provides an opinion on the fairness of presentation, the adequacy of design, and the operating effectiveness of key application and general computer controls that are relevant to audits of user organization financial statements. As a result, this audit precludes the need for multiple audits of DCPS controls previously performed by user organizations to plan or conduct financial statement and performance audits. This audit will also provide, in a separate audit report, recommendations to management for correction of identified control deficiencies. Effective internal control is critical to achieving reliable information for all management reporting and decision-making purposes.

---

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

---





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

September 28, 2006

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 the Defense Civilian Pay System Controls Placed in Operation and  
Tests of Operating Effectiveness for the Period July 1, 2005, through  
June 30, 2006

We have examined the accompanying description of the general computer and application controls related to the Defense Civilian Pay System (DCPS). DCPS is owned by Defense Finance and Accounting Service (DFAS) and maintained and supported by DFAS technical support elements and Defense Information Systems Agency (DISA). As such, the DCPS general computer and application controls are managed by both DISA and DFAS. Our examination 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 the controls relate 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 June 30, 2006.

The control objectives were specified by the DoD Office of Inspector General (OIG). We performed our examination 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 in the circumstances to obtain a reasonable basis for rendering our opinion.

The accompanying description includes only those application control objectives and related controls resident at the Charleston, South Carolina; Pensacola, Florida; and Denver, Colorado, payroll offices. DCPS processes data from DoD and external customers through the use of approximately 109 interface systems. Examples of those interface systems include the Defense Civilian Personnel Data System, Automated Time and Attendance and Production System, Automated Disbursing System, and the Defense Joint Accounting System. The accompanying description does not include control objectives and general and application controls related to the systems that interface with



DCPS. Our examination did not extend to the controls resident at the National Security Agency (NSA) payroll office and related systems that interface with DCPS.

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

DCPS began processing pay for the Environmental Protection Agency (EPA) on May 25, 2006. Therefore, our examination only covered controls in place for EPA payroll processing for the period May 26, 2006, through June 30, 2006.

Our examination was conducted for the purpose of forming an opinion on the description of the DCPS general and application controls at DFAS and DISA (Section II). Information about business continuity plans and procedures at DFAS and DISA, as provided by those organizations and included in Section IV, is presented to provide 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 examination of the aforementioned description of controls at DFAS and DISA. Accordingly, we do not express an opinion on the description of the business continuity plans and procedures provided by DFAS and DISA.

In our opinion, the accompanying description of the DCPS general computer and application controls at DFAS and DISA (Section II) presents fairly, in all material respects, the relevant aspects of the controls at DFAS and DISA that had been placed in operation as of June 30, 2006. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and users applied those aspects of internal control contemplated in the design of the controls at DFAS and DISA.

In addition to the procedures that we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specified controls, listed in Section III, to obtain evidence about their effectiveness in meeting the related control objectives described in Section III during the period of July 1, 2005, through June 30, 2006. The specific control objectives, controls, and the nature, timing, extent, and results of the tests are documented in Section III. This information has been provided 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 risk for the user organizations.

In performing our examination, we identified the following exceptions to our tests of operating effectiveness related to the controls described in the "Description of DCPS Operations and Controls Provided by DFAS and DISA" (Section II).

#### **DCPS User Access**

DFAS requires a DD Form 2875, "System Access Authorization Request," (SAAR) form be completed by every DCPS user. The SAAR form documents user access and must be signed by a supervisor indicating that such access has been approved.

Upon examining a selection of 45 DCPS payroll office user's SAAR forms, we identified the following exceptions.

- DFAS could not locate 3 of 45 SAAR forms selected for review.

- DCPS user access did not match the access authorized on 1 of 42 SAAR forms examined.
- The completion date of the initial computer-based security training was not included on 2 of 42 SAAR forms examined.

Upon examining a selection of 45 DCPS non-payroll office users' SAAR forms, we identified the following exceptions.

- DFAS could not locate 4 of 45 SAAR forms selected for review.
- The completion date of the initial computer-based security training was not included on 4 of 41 SAAR forms examined.
- The supervisor's signature was not included on 2 of 41 SAAR forms examined.

As a result, the following control objectives that rely on this control may not have been fully achieved during the period of July 1, 2005, through June 30, 2006:

"Controls provide reasonable assurance that only valid and accurate changes are made to the payroll master files and payroll withholding tables."

"Controls provide reasonable assurance that changes to the payroll master files and withholding tables are authorized, input, and processed timely."

"Controls provide reasonable assurance that current- or prior-period adjustments to employee's pay, including employee debt, tax deductions, or deductions not taken, are reported, reconciled, and approved."

"All application users are appropriately identified and authenticated. Access to the application and output is restricted to authorized users for authorized purposes."

"Controls provide reasonable assurance that data transmissions in DCPS from user organizations are authorized, complete, accurate, and secure."

### **Monitoring DCPS Error Reports**

The DCPS Personnel Interface Invalid Report (Report No. P6606R01) is a key control for monitoring and resolving DCPS interface processing errors. We selected a sample of 45 Personnel Interface Invalid Reports generated between July 1, 2005, and June 30, 2006, at each payroll office to confirm whether the reports were consistently annotated to indicate processing exceptions were resolved. Also, we selected 16 additional Personnel Interface Invalid Reports (the 16 reports represented all reports processed during the reporting period) for the ZPA database at the DFAS Denver payroll office.

At the DFAS Denver payroll office, we examined 61 Personnel Interface Invalid Reports generated between July 1, 2005, and June 30, 2006, for the OMA and ZPA pay databases. We identified that:

- of the 61 Personnel Interface Invalid Reports examined, 36 reports contained transactions that were not annotated by payroll office technicians with sufficient detail documenting how errors were resolved and

- of the 61 Personnel Interface Invalid Reports examined, 3 reports did not include the date that actions were taken by payroll office technicians.

At the DFAS Charleston payroll office, Personnel Interface Invalid Reports generated between July 1, 2005, and February 13, 2006, had not been annotated and could not be provided for auditor review. Subsequently, DFAS Charleston annotated the reports in hardcopy after exhausting all efforts to implement an electronic solution. Therefore, the sample included all Personnel Interface Invalid Reports processed during February 14, 2006, through June 30, 2006. We examined 45 Personnel Interface Invalid Reports from the ZFA, ZFR, ZGT, ZLO, ZPD, and ZPH pay databases from this period. We identified that:

- of the 45 Personnel Interface Invalid Reports selected for review, 3 could not be provided because they were removed from Computer Associates Doc View system and
- of the 42 Personnel Interface Invalid Reports examined, all of the reports included transactions that were not signed, dated, or annotated by payroll office technicians with sufficient detail documenting how errors were resolved.

At the DFAS Pensacola payroll office, we selected a sample of 45 Personnel Interface Invalid Reports from the CP1 and ZKA pay databases. However, DFAS Pensacola could not locate one Personnel Interface Invalid Report from the CP1 pay database; therefore, we examined 23 Personnel Interface Invalid Reports from the CP1 pay database, and 21 Personnel Interface Invalid Reports from the ZKA pay database. We identified that all 44 Personnel Interface Invalid Reports examined contained transactions that were not signed, dated, or annotated by payroll office technicians with sufficient detail documenting whether all errors were resolved and how those errors were resolved. As a result, the following control objectives that rely on this control may not have been fully achieved during the period of July 1, 2005, through June 30, 2006:

“Controls provide reasonable assurance that changes to the payroll master files and withholding tables are authorized, input, and processed timely.”

“Controls provide reasonable assurance of the integrity and reliability of DCPS data for financial reporting purposes.”

“Controls provide reasonable assurance that fiscal year-end, leave-year-end and calendar year-end processing occurs in accordance with established Government-wide and agency guidelines.”

“Controls are reasonable to ensure that transmissions from interfacing systems are subjected to the payroll system edits, validations and error-correction procedures.”

### **Monitoring and Tracking DCPS Remedy Tickets**

DCPS payroll office personnel use Remedy software to track and monitor DCPS-related processing issues, as well as administrative requests, such as granting and removing user access within DCPS. Upon inspecting a sample of 45 Remedy tickets processed by the three payroll offices, we identified the following exceptions.

- DFAS Denver payroll office did not process 2 of 45 Remedy tickets examined within the required time frame.
- DFAS Charleston payroll office did not process 6 of 45 Remedy tickets examined within the required time frame.
- DFAS Pensacola payroll office did not process 3 of 45 Remedy tickets examined within the required time frame.

In addition, we observed that the Remedy tickets were not sequentially numbered because Remedy tickets used for testing purposes were deleted from the system. As a result, the following control objectives that rely on this control may not have been fully achieved during the period of July 1, 2005, through June 30, 2006:

“Controls provide reasonable assurance that changes to the payroll master files and withholding tables are authorized, input, and processed timely.”

“Controls provide reasonable assurance that current- or prior-period adjustments to employee's pay, including employee debt, tax deductions, or deductions not taken, are reported, reconciled, and approved.”

### **DCPS Database Access**

DFAS Technical Support Organization Pensacola (TSOPE) Database Administrators could make changes directly to payroll data recorded in the DCPS Integrated Database Management System (IDMS) by using a Data Manipulation Language Online tool. Although those changes would then be recorded in an audit log, TSOPE management would not review those regularly to determine whether the changes were appropriate and had been approved. We also identified three active user accounts on the IDMS user access list; however, those accounts were not associated with personnel who needed that type of access. Specifically, one account was for an individual no longer employed by DFAS TSOPE, one account was a duplicate account, and one account was for an individual that no longer required that level of access. As a result, the following control objectives that rely on this control may not have been fully achieved during the period of July 1, 2005, through June 30, 2006:

“Access settings have been implemented in accordance with the access authorizations established by the resource owners.”

“Access to program libraries is restricted to appropriate personnel to ensure that the movement of programs and data among libraries is controlled.”

### **DCPS Interfaces**

All DCPS interfaces should have a signed memorandum of agreement documenting key information, including impacted parties, interconnection requirements, points of contact, security requirements, technical platform information, interface file information, and designated signatories. However, 79 of 109 DCPS interfaces did not have a documented memorandum of agreement in place. As a result, the control objective “Owners determine disposition and sharing of data” that relies on this control may not have been fully achieved during the period of July 1, 2005, through June 30, 2006.

## **DCPS System Access**

The Defense Enterprise Computing Center (DECC) System Management Center (SMC) Mechanicsburg requires that a SAAR form be completed before DECC SMC Mechanicsburg grants access to DCPS. The SAAR form indicates the justification of DCPS access and must be approved and signed by a supervisor before DECC SMC Mechanicsburg grants access to the DCPS operating system. Upon inspecting a sample of 45 SAAR forms, we identified the following exceptions.

- Justification documenting why access to DCPS was required by DECC SMC Mechanicsburg personnel was not included on 4 of 45 SAAR forms examined.
- The user's organization was not included on 1 of 45 SAAR forms examined.

DFAS TSOPE technical support personnel have unrestricted access to flat files that contain DCPS customer data sent for processing or DCPS files that contain payroll, bank account, and other personal information. The technical support personnel have the ability to edit data within flat files. Although audit logs record the date, time, and user identification of the person accessing the flat files, the audit log does not identify the nature of the change. As a result, the following control objectives that rely on this control may not have been fully achieved during the period of July 1, 2005, through June 30, 2006:

“Access is restricted to data files and software programs.”

“Access settings have been implemented in accordance with the access authorizations established by the resource owners.”

“Discretionary access controls are a sufficient information assurance (IA) mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rule.”

“Individuals requiring access to sensitive information are processed for access authorization in accordance with DoD personnel security policies.”

## **DCPS Application Change Controls**

DFAS is required to assess the impact changes to the DCPS application will have on IA requirements prior to the change being moved into the production environment. Upon inspecting 45 randomly selected changes to the system, we identified 26 DCPS application changes that were not assessed for IA impact. As a result, the control objective “Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation” that relies on this control may not have been fully achieved during the period of July 1, 2005, through June 30, 2006.

## **DCPS System Readiness Reviews**

The DISA Field Security Operations (FSO) performs periodic System Readiness Reviews (SRRs) on DISA operating systems to assess compliance with DoD information security standards. DISA policy requires the FSO to perform an SRR every 3 years. However, the FSO has not conducted an SRR within the last 3 years on the mainframe Logical Partition (LPAR) that houses the DCPS application. As a result, the following control

objectives that rely on this control may not have been fully achieved during the period of July 1, 2005, through June 30, 2006:

“Risks are periodically assessed.”

“Management ensures that corrective actions are effectively implemented.”

“A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place.”

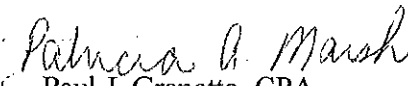
In our opinion, except for the deficiencies in operating effectiveness noted in the preceding paragraphs, the controls that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section III were achieved during the period of July 1, 2005, through June 30, 2006. However, the scope of our engagement did not include tests to determine whether control objectives not listed in Section III were achieved; accordingly, we express no opinion on the achievement of control objectives not included in Section III.

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 June 30, 2006, and information about tests of their operating effectiveness covers the period of July 1, 2005, through June 30, 2006. Any projection of such information to the future 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 might not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

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

By direction of the Deputy Inspector General for Auditing:

  
for Paul J. Granetto, CPA  
Assistant Inspector General  
Defense Financial Auditing  
Service



---

**Section II: Description of DCPS Operations and Controls  
Provided by DFAS and DISA**

---





## **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. DCPS began paying the EOP in 1998. The President's Management Agenda e-Payroll initiative requires DFAS, as one of four federal payroll providers, to service the entire executive branch of the Federal government. DFAS began processing payroll for the Department of Energy in 2003, the Department of Health and Human Services in 2005, and the EPA in 2006. As of June 30, 2006, DCPS currently processes pay for approximately 789,000 employees.

The DCPS program mission is to process payroll for 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 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.

Approximately 2,900 payroll processing personnel at three DFAS payroll offices located in Pensacola, Florida; Charleston, South Carolina; and Denver, Colorado use DCPS. DCPS is also used at NSA.<sup>1</sup> Additional users include Customer Service Representatives at customer activities and sites. The three DFAS payroll offices process payroll for all DoD civilians. The Pensacola payroll office processes EOP payroll; the Charleston payroll office processes Departments of Energy and Health and Human Services payroll; and the Denver payroll office processes EPA payroll.

### **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 Services Product Line and the System Management Office (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. The Civilian Pay Services Product Line and the System Management Office (SMO) are responsible for requirements management, functional analysis, information assurance, and user documentation processes. TSOPE provides DCPS software engineering, production support, and customer service. Within TSOPE, several groups provide DCPS support. The Software Engineering Division provides

---

<sup>1</sup>The NSA payroll office is not included in the scope of this "Description of DCPS Operations and Controls Provided by DFAS and DISA."

technical design, programming, unit testing, and system documentation. The Software Test and Evaluation Division perform integration testing and evaluation processes. The Project Support Division provides system software, telecommunication, computer resource tools, and database support. The DCPS Software Quality Assurance Office 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 DECC SMC Mechanicsburg, 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 or generating Leave and Earnings Statements).
- *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 and timesheets) at customer locations. The components are largely customer-owned and operated, and include local area networks, 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 computers or workstations maintained by the Defense Automated Printing Service at sites located in various U.S. and overseas geographical regions.

The two tiers of the DCPS architecture are connected by DoD-maintained networks composed of Internet Protocol-based (for example, the Non-Classified Internet Protocol Router Network) and Systems Network Architecture-based (leased line) services. Those networks connect DCPS to a wide variety of external, non-DCPS sites (mainframes, mid-tiers, and personal computers) 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, Federal Reserve Board, Thrift Savings Plan (TSP), Department of the Treasury, and non-DoD users such as the Departments of Energy and Health and Human Services, EOP, and EPA.

The main technical components of DCPS include the following attributes.

- DCPS is housed in a separate logical domain on an IBM Z900 mainframe computer located at DECC SMC Mechanicsburg.
- The IBM mainframe operating system software is Z/OS release 1.4.
- DCPS is written in Common Business Oriented II language (COBOL).

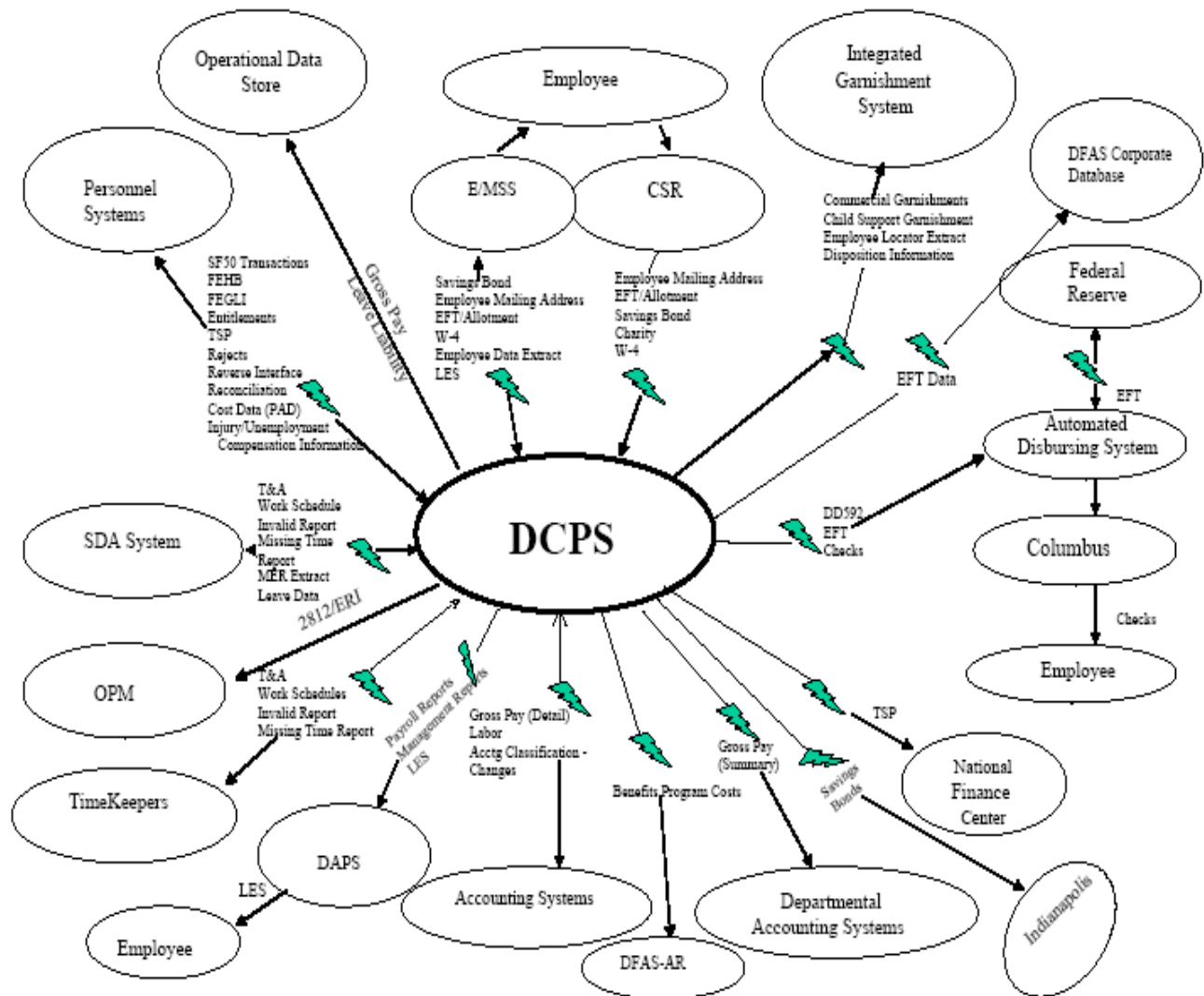
- First point of entry security protection mechanisms are provided by Access Control Facility 2 (ACF2).
- DECC SMC Mechanicsburg provides four web servers that service all applications that support DCPS. Those servers accept the users' secure web requests by supplying a menu screen with options for each application to the DCPS logon screen, where individuals enter their ACF2 login user identification and passwords.
- Third-party software packages are used for DCPS process scheduling and monitoring.

The payroll offices and associated Customer Service Representatives have access to DCPS through dedicated leased lines, various DoD networks, and through Secure Web Access. Secure Web Access enables secure transaction processing across the Non-Classified Internet Protocol Router Network. DISA is in the process of transitioning Secure Web Access to the Mainframe Internet Access Portal, which is centrally managed by the Communications Control Center, Montgomery, Alabama. IBM's Host-on-Demand was used to establish the Secure Web Access infrastructure. 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. 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, 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. 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 DECC SMC Mechanicsburg is "MAC II."

### **DCPS Data Flow**

The following figure depicts the flow of data to and from DCPS as of April 2005. 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.



## Overview of System Interfaces

DCPS is a combination of online and batch programs that support the requirements of a biweekly payroll process for approximately 789,000 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 online workload and to obtain labor data. However, the focal point of the system is the biweekly process. Non-biweekly process functions occur monthly, quarterly, annually, or as required, and are in support of, or a result of, multiple biweekly pay cycles. DCPS supports a standard personnel interface, decentralized time and attendance reporting, and the Customer Service Representatives structure.

DCPS accepts input from three primary areas: Customer Service Representatives, timekeepers, and personnel offices. DCPS receives or creates data for approximately 109 interface systems 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 file 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 DECC SMC Mechanicsburg, Pennsylvania. DECC SMC Mechanicsburg 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 Manager prior to gaining access to DCPS. The Information

Security 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 is and what the Terminal Area Security Officer's 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 do not require any specific level of prior security clearance before a candidate can become an employee.

### *DECC SMC Mechanicsburg*

The security manager is responsible for processing and vetting new employees and contractors who are given access to DECC SMC Mechanicsburg 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. The contracting officer is responsible for confirming that all contractors are assigned to a valid contract, and have been approved to work at DECC SMC Mechanicsburg.

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 SAAR form 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. Those reports are reviewed each pay period 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. DCPS technicians perform remedial action, such as additions, deletions, or changes to customer data, as necessary. In addition, several organizations within DoD perform monitoring activities associated with DCPS-related internal controls.

### **DISA OIG**

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.

## **FSO**

The 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 DECC SMC Mechanicsburg management and does not maintain or configure DCPS.

## **DoD OIG**

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, establishes 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 nontechnical 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 process, 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 signed on July 15, 2005, and is valid for three years. The DECC SMC Mechanicsburg enclave SSAA was signed on October 26, 2005, and is valid for three years. The DCPS application Authority to Operate, July 29, 2005, is on file with the CDB3 Information Assurance Manager. The DCPS Authority to Operate will be included in the annual SMC Mechanicsburg Unclassified Enclave SSAA package update that is submitted to the DISA Designated Approval Authority.



## **D. Risk Assessment**

The DITSCAP process, 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 yearly basis. Personnel from DFAS TSOPE and DECC SMC Mechanicsburg 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 Departments of Energy and Health and Human Services, EOP, and EPA. Payroll processing includes data from approximately 109 interface systems. 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 SMC Mechanicsburg is documented through a Service-Level agreement that includes various DFAS and DECC SMC Mechanicsburg points of contact and liaisons that should be used when DCPS issues arise. DECC SMC Mechanicsburg 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 payroll offices meet weekly to discuss DCPS processing issues. The Configuration Control Board (CCB), comprised of 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 TSOPE for resolution.

## **F. Control Activities**

The DCPS control objectives and related control activities are included in Section III of this report, "Information Provided by the Service Auditor," to eliminate the redundancy that would result from listing them in this section and repeating them 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 the following events occur.

- The Information Systems Security Officer located at the payroll offices is notified of all terminated employees with access to DCPS.
- The local Human Resource Office is notified of all terminated employees to ensure that those 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.
- All pseudo Social Security Numbers (if created) have been authorized by appropriate user organization personnel and, if necessary, are accurately tied to a primary and valid Social Security Number.
- 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.
- 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**

---



## **A. Scope Limitations**

The control objectives documented in this section were specified by the DoD OIG. As described in the prior section (Section II), DCPS interfaces with many systems. The controls described and tested within 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 input, processing, and output controls within those interface systems.

## 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	Controls provide reasonable assurance that only valid and accurate changes are made to the payroll master files and payroll withholding tables.	Policies and procedures are documented to describe how only valid and accurate changes are made to the payroll master files and payroll withholding tables.	Read policies and procedures and inquired with appropriate personnel to confirm that only valid changes are made to the payroll master files and payroll withholding tables.	No relevant exceptions noted.
		Payroll master file and withholding data tables are periodically reviewed by supervisory personnel for accuracy and ongoing pertinence.	Inquired with appropriate personnel and inspected online queries (OLQs) and summary reports to confirm that master files and withholding tables were periodically reviewed by supervisory personnel for accuracy and ongoing pertinence.	No relevant exceptions noted.
		Programmed validation and edit checks identify erroneous data.	Inquired with appropriate personnel and observed programmed validation and edit checks to confirm they existed.	No relevant exceptions noted.
		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 45 access forms to confirm that the master file is restricted to authorized personnel.	<p><u>DFAS Denver</u></p> <p><u>Payroll Office Users</u></p> <p>Of the 12 SAAR forms selected for review, 1 form could not be located.</p> <p><u>Non-Payroll Office Users</u></p> <p>Of the 15 SAAR forms inspected, 1 form did not include the completion date of the initial computer-based security training. In addition, 1 of the 15 SAAR forms inspected did not include a supervisor's signature.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>The ZPA database included 42 users with supervisory-level access.</p> <p><u>DFAS Pensacola</u> <u>Payroll Office Users</u></p> <p>Of the nine SAAR forms selected for review, one form could not be located. Of the eight SAAR forms inspected, two forms did not include the completion date of the initial computer-based security training.</p> <p><u>Non-Payroll Office Users</u></p> <p>Of the 26 SAAR forms selected for review, 4 forms could not be located. Of the 22 SAAR forms inspected, 3 forms did not include the completion date of the initial computer-based security training. In addition, 2 of the 22 SAAR forms inspected did not include the supervisor's signature.</p> <p><u>DFAS Charleston</u> <u>Payroll Office Users</u></p> <p>Of the 24 SAAR forms selected for review, 1 form could not be located. Of the 23 SAAR forms inspected, 1 form did not match the level of authorized access actually granted.</p> <p>The Charleston payroll office had 133 DCPS users with access to update time and attendance and Master Employee data.</p> <p><u>Non-Payroll Office Users</u></p> <p>No relevant exceptions noted.</p>



No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		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>Inquired with appropriate personnel and observed the process for making tax changes to the payroll withholding tables and master files after being compared to authorized source documents by supervisory personnel to ensure that they were tested and approved.</p> <p>Inquired with appropriate personnel and observed the imaging process to confirm that inputs are compared to authorized Imaging documents to ensure that they were input accurately.</p>	No relevant exceptions noted.
2	Controls provide reasonable assurance that changes to the payroll master files and withholding tables are authorized, input, and processed timely.	Policies and procedures are documented to describe how changes to the payroll master files and withholding tables are authorized, input, and processed timely.	Inquired with appropriate personnel and read policies and procedures to confirm that changes to the payroll master files and withholding tables are authorized, input, and processed timely.	No relevant exceptions noted.
Changes to the payroll master file and withholding table data are logged in numerous reports including the Master Employee Add/Change/Delete Report and reviewed by supervisory personnel to ensure that all requested changes are processed timely.		Inquired with appropriate personnel and inspected OLQs and summary reports to confirm that changes to the payroll master file and table data are logged and reviewed by supervisory personnel.	No relevant exceptions noted.	
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; key source documents require signatures from supervisory personnel.		<p>Inquired with appropriate personnel and inspected a random sample of 45 Remedy tickets to confirm that:</p> <ol style="list-style-type: none"> <li>1) tickets are pre-numbered,</li> <li>2) the sequence is accounted for so that the forms are accounted for timely,</li> <li>3) access to the source documents is controlled,</li> </ol>	<p><u>DFAS Denver</u></p> <p>Of the 45 Remedy tickets inspected, 2 tickets were not completed within the required 3-10 day time frame.</p> <p><u>DFAS Pensacola</u></p> <p>Of the 45 Remedy tickets inspected, 3 tickets were not completed within the required 3-10 day time frame.</p>	

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			<p>4) key source documents require signatures from supervisory personnel, and</p> <p>5) tickets are completed within the required time frame.</p>	<p><u>DFAS-Charleston</u></p> <p>Of the 45 Remedy tickets inspected, 6 tickets were not completed within the required 3-10 day time frame.</p> <p><u>All Payroll Offices</u></p> <p>Remedy tickets were not sequentially numbered. Remedy tickets used for testing purposes were deleted. Documentation was not maintained for these tickets.</p>
		<p>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 random sample of 45 Personnel Interface Invalid Reports for erroneous transactions to confirm that items are investigated and resolved timely.</p> <p>Selected a random sample of 45 Personnel Interface Invalid Reports for the OMA pay database. In addition, the ZPA pay database only processed data for two pay periods, therefore, we reviewed all 16 Personnel Interface Invalid Reports during that period at DFAS Denver. As a result, 61 Personnel Interface Invalid Reports were selected for review at DFAS Denver.</p> <p>Selected a random sample of 45 Personnel Interface Invalid Reports beginning on February 14, 2006, at DFAS Charleston.</p>	<p><u>DFAS Denver</u></p> <p><u>OMA Pay Database</u></p> <p>Of the 45 Personnel Interface Invalid Reports inspected, 3 reports did not include a date indicating when actions to correct the errors had been completed. In addition, 35 of the 45 Personnel Interface Invalid Reports inspected did not include annotations indicating how the errors were corrected.</p> <p><u>ZPA Pay Database</u></p> <p>Of the 16 Personnel Interface Invalid Reports inspected, 1 report did not include annotations indicating how the errors were corrected.</p> <p><u>DFAS Pensacola</u></p> <p>Of the 45 Personnel Interface Invalid Reports selected for review, 1 report could not be located. Of the 44 Personnel Interface Invalid Reports inspected, 25 reports were annotated; however, sufficient</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>detail did not exist to determine whether all errors within the report were resolved.</p> <p>In addition, 19 of the 44 Personnel Interface Invalid Reports inspected were annotated in Microsoft Word, but did not include the annotator's signature or date of annotation.</p> <p><u>DFAS Charleston</u></p> <p>Personnel Interface Invalid Reports were neither annotated, nor available for review July 1, 2005, through February 13, 2006.</p> <p>Of the 45 Personnel Interface Invalid Reports selected for review, 3 reports could not be provided. None of the 42 Personnel Interface Invalid Reports inspected included a signature, date, and annotations indicating how the errors were corrected.</p>
		<p>The ability to view, modify, or transfer information contained in the payroll master files is restricted to authorized personnel.</p>	<p>Inquired with appropriate personnel and inspected a random sample of 45 access forms to confirm that the master file is restricted to authorized personnel.</p>	<p><u>DFAS Denver</u></p> <p><u>Payroll Office Users</u></p> <p>Of the 12 SAAR forms selected for review, 1 form could not be located.</p> <p><u>Non-Payroll Office Users</u></p> <p>Of the 15 SAAR forms inspected, 1 form did not include the completion date of the initial computer-based security training. In addition, 1 of the 15 SAAR forms inspected did not include a supervisor's signature.</p> <p>The ZPA database included 42 users with supervisory-level access.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p><u>DFAS Pensacola</u></p> <p><u>Payroll Office Users</u></p> <p>Of the nine SAAR forms selected for review, one form could not be located. Of the eight SAAR forms inspected, two forms did not include the completion date of the initial computer-based security training.</p> <p><u>Non-Payroll Office Users</u></p> <p>Of the 26 SAAR forms selected for review, 4 forms could not be located. Of the 22 SAAR forms inspected, 3 forms did not include the completion date of the initial computer-based security training. In addition, 2 of the 22 SAAR forms inspected did not include the supervisor's signature.</p> <p><u>DFAS Charleston</u></p> <p><u>Payroll Office Users</u></p> <p>Of the 24 SAAR forms selected for review, 1 form could not be located. Of the 23 SAAR forms inspected, 1 form did not match the level of authorized access actually granted.</p> <p>The Charleston payroll office had 133 DCPS users with access to update time and attendance and Master Employee data.</p> <p><u>Non-Payroll Office Users</u></p> <p>No relevant exceptions noted.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
3	Controls provide reasonable assurance that payroll processing is accurate and recorded in the proper period.	Policies and procedures are documented to describe how payroll processing is accurate and recorded in the proper period.	Inquired with appropriate personnel and read policies and procedures to confirm that payroll processing is accurate and recorded in the appropriate period.	No relevant exceptions noted.
		Compliance with the payroll disbursement processing schedule is monitored by management.	Inquired with appropriate personnel and inspected pay processing schedules and observed payroll disbursement process to confirm the monitoring of payroll disbursement processing schedule by management.	No relevant exceptions noted.
		The detailed "592" payroll reconciliation shows that 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 reconciled items are investigated and cleared on a timely basis by supervisors prior to disbursement.	<p>Inquired with appropriate personnel and examined a sample of 26 "592" reconciliations for each database to confirm the following conditions exist.</p> <ol style="list-style-type: none"> <li>1) The detailed payroll reconciliation shows that 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.</li> <li>2) Each "592" reconciliation is approved by management prior to disbursement.</li> <li>3) Reconciled items are investigated and cleared on a timely basis by supervisors prior to disbursement.</li> </ol>	<p><u>DFAS Pensacola</u> Of the 26 "592" reconciliation reports inspected, 1 report did not include a preparer's signature and date. In addition, the Withholdings for Benefits report did not have a Certifying Officer's signature and date. However, DFAS Denver maintained a signed copy of the "592" reconciliation report that they processed during contingency operations on behalf of DFAS Pensacola.</p> <p><u>DFAS Denver</u> No relevant exceptions noted.</p> <p><u>DFAS Charleston</u> No relevant exceptions noted.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		Summary payroll reports (including OLQs of total disbursements, retirement, TSP, bonds, and other withholdings) are reviewed and approved by management prior to disbursement.	Inquired with appropriate personnel and inspected summary reports and OLQs to confirm they are reviewed and approved by management prior to disbursement.	No relevant exceptions noted.
4	Controls provide reasonable assurance that disbursed payroll (including compensation and withholding) is accurately calculated and recorded.	Policies and procedures are documented to describe how disbursed payroll (including compensation and withholding) is calculated and recorded.	Inquired with appropriate personnel and read policies and procedures to confirm that disbursed payroll is accurately calculated and recorded.	No relevant exceptions noted.
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 reconciled items are investigated and cleared on a timely basis by supervisory personnel prior to disbursement.		<p>Inquired with appropriate personnel and examined a sample of 26 "592" reconciliations for each database to confirm that the following conditions exist.</p> <ol style="list-style-type: none"> <li>1) The detailed payroll reconciliation shows that 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.</li> <li>2) Each "592" reconciliation is approved by management prior to disbursement.</li> <li>3) Reconciled items are investigated and cleared on a timely basis by supervisory personnel prior to disbursement.</li> </ol>	<p><u>DFAS Pensacola</u> Of the 26 "592" reconciliation reports inspected, 1 report did not include a preparer's signature and date. In addition, the Withholdings for Benefits report did not have a Certifying Officer's signature and date. However, DFAS Denver maintained a signed copy of the "592" reconciliation report that they processed during contingency operations on behalf of DFAS Pensacola.</p> <p><u>DFAS Denver</u> No relevant exceptions noted.</p> <p><u>DFAS Charleston</u> No relevant exceptions noted.</p>	

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		Summary payroll reports (including OLQs of total disbursements, retirement, TSP, bonds, and other withholdings) are reviewed and approved by management prior to disbursement.	Inquired with appropriate personnel and inspected summary reports and OLQs to confirm they are reviewed and approved by management prior to disbursement.	No relevant exceptions noted.
		DCPS performs limit and reasonableness checks on employee earnings.	Inquired with appropriate personnel and inspected the limit and reasonableness report to confirm reasonableness checks are performed on employee earnings.	No relevant exceptions noted.
		Programmed validation and edit checks identify erroneous data.	Observed the input of new employees into DCPS to confirm that programmed validation and edit checks identify erroneous data entered directly into DCPS.	No relevant exceptions noted.
5	Controls provide reasonable assurance that only valid, authorized employees are paid and that payroll is disbursed to appropriate employees.	Policies and procedures are documented to describe how only valid, authorized employees are paid and that payroll is disbursed to appropriate employees.	Inquired with appropriate personnel and read policies and procedures to confirm that only valid, authorized employees are paid and that payroll is disbursed to appropriate employees.	No relevant exceptions noted.
		OLQs and summary reports (including the Master Employee Add/Change/Delete Report) are periodically reviewed by supervisory personnel to determine if the master files remain accurate and pertinent.	Inquired with appropriate personnel and inspected OLQs and summary reports to confirm that master files and withholding tables are periodically reviewed by supervisory personnel.	No relevant exceptions noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		<p>Departmental managers periodically review listings (including the Personnel/Payroll Reconciliation or Control of Hours Report) of current employees within their departments and notify the personnel department of necessary changes. All payroll queries are followed up by persons independent of the payroll preparation and disbursement process.</p>	<p>Inquired with appropriate personnel and inspected the Personnel/Payroll Reconciliation or Control of Hours Reports to confirm that they are sent to management for review of employee listings and notification to personnel department of changes.</p>	<p>No relevant exceptions noted.</p>
		<p>The detailed “592” payroll reconciliation shows that 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 reconciled items are investigated and cleared on a timely basis by supervisory personnel prior to disbursement.</p>	<p>Inquired with appropriate personnel and examined a sample of 26 “592” reconciliations for each database to confirm that the following conditions exist.</p> <ol style="list-style-type: none"> <li>1) The detailed payroll reconciliation shows that 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.</li> <li>2) Each “592” reconciliation is approved by management prior to disbursement.</li> <li>3) Reconciled items are investigated and cleared on a timely basis by supervisory personnel prior to disbursement.</li> </ol>	<p><u>DFAS Pensacola</u> Of the 26 “592” reconciliation reports inspected, 1 report did not include a preparer’s signature and date. In addition, the Withholdings for Benefits report did not have a Certifying Officer’s signature and date. However, DFAS Denver maintained a signed copy of the “592” reconciliation report that they processed during contingency operations on behalf of DFAS Pensacola.</p> <p><u>DFAS Denver</u> No relevant exceptions noted.</p> <p><u>DFAS Charleston</u> No relevant exceptions noted.</p>
		<p>Summary payroll reports (including OLQs of total disbursements, retirement, TSP, bonds, and other withholdings) are reviewed and approved by management prior to disbursement.</p>	<p>Inquired with appropriate personnel and inspected summary reports and OLQs to confirm that they are reviewed and approved by management prior to disbursement.</p>	<p>No relevant exceptions noted.</p>



No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		Only authorized personnel have the ability to disburse payroll.	Inquired with the appropriate personnel, observed the disbursement of payroll, and inspected a random sample of DCPS user profiles for disbursement privileges to confirm that only authorized personnel have the ability to disburse payroll.	No relevant exceptions noted.
6	Controls provide reasonable assurance of the integrity and reliability of DCPS data for financial reporting purposes.	Policies and procedures are documented to describe how management ensures that controls provide reasonable assurance of the integrity and reliability of DCPS data for financial reporting purposes.	Inquired with appropriate personnel and read policies and procedures to confirm that controls provide reasonable assurance of the integrity and reliability of DCPS data for financial reporting purposes.	No relevant exceptions noted.
		Payroll transactions at the end of a payroll cycle are reconciled by supervisors to ensure complete and consistent recording in the appropriate accounting period.	Inquired with appropriate personnel and examined a sample of 26 "592" payroll reconciliations at the end of a payroll cycle to confirm they are reconciled to ensure complete and consistent recording in the appropriate accounting period.	No relevant exceptions noted.
		Error reports (for example, the Personnel Interface Invalid Report), and error warnings show rejected transactions with error messages that have clearly understandable corrective actions for each type of error.	Inquired with appropriate personnel and inspected error warnings and a random sample of 45 Personnel Interface Invalid Reports to confirm that they show rejected transactions with error messages that have clearly understandable corrective actions for each type of error.  Selected a random sample of 45 Personnel Interface Invalid Reports for the OMA pay database. In addition, the ZPA pay database only processed data for two pay periods, therefore, we reviewed all 16 Personnel Interface Invalid Reports during that period at DFAS Denver. As a result, 61 Personnel Interface	<u>DFAS Denver</u> <u>OMA Pay Database</u> Of the 45 Personnel Interface Invalid Reports inspected, 3 reports did not include a date indicating when actions to correct the errors had been completed. In addition, 35 of the 45 Personnel Interface Invalid Reports inspected did not include annotations indicating how the errors were corrected.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			<p>Invalid Reports were selected for review at DFAS Denver.</p> <p>Selected a random sample of 45 Personnel Interface Invalid Reports beginning on February 14, 2006, at DFAS Charleston.</p>	<p><u>ZPA Pay Database</u></p> <p>Of the 16 Personnel Interface Invalid Reports inspected, 1 report did not include annotations indicating how the errors were corrected.</p> <p><u>DFAS Pensacola</u></p> <p>Of the 45 Personnel Interface Invalid Reports selected for review, 1 report could not be located. Of the 44 Personnel Interface Invalid Reports inspected, 25 reports were annotated; however, sufficient detail did not exist to determine whether all errors within the report were resolved.</p> <p>In addition, 19 of the 44 Personnel Interface Invalid Reports inspected were annotated in Microsoft Word, but did not include the annotator's signature or date of annotation.</p> <p><u>DFAS Charleston</u></p> <p>Personnel Interface Invalid Reports were neither annotated, nor available for review July 1, 2005, through February 13, 2006.</p> <p>Of the 45 Personnel Interface Invalid Reports selected for review, 3 reports could not be provided. None of the 42 Personnel Interface Invalid Reports inspected included a signature, date, and annotations indicating how the errors were corrected.</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, and each erroneous transaction is annotated with codes indicating the type of data error, the date and time the transaction was processed and the error identified, and the identity of the user who originated the transaction.</p>	<p>Inquired with the appropriate personnel and inspected the Personnel Interface Invalid Report of rejected data to confirm that the rejected data are automatically written on an automated error suspense file and held until corrected by payroll technicians, and each erroneous transaction is annotated with codes indicating the type of data error, the date and time the transaction was processed and the error identified, and the identity of the user who originated the transaction.</p> <p>Selected a random sample of 45 Personnel Interface Invalid Reports for the OMA pay database. In addition, the ZPA pay database only processed data for two pay periods, therefore, we reviewed all 16 Personnel Interface Invalid Reports during that period at DFAS Denver. As a result, 61 Personnel Interface Invalid Reports were selected for review at DFAS Denver.</p> <p>Selected a random sample of 45 Personnel Interface Invalid Reports beginning on February 14, 2006, at DFAS Charleston.</p>	<p><u>DFAS Denver</u> <u>OMA Pay Database</u></p> <p>Of the 45 Personnel Interface Invalid Reports inspected, 3 reports did not include a date indicating when actions to correct the errors had been completed. In addition, 35 of the 45 Personnel Interface Invalid Reports inspected did not include annotations indicating how the errors were corrected.</p> <p><u>ZPA Pay Database</u></p> <p>Of the 16 Personnel Interface Invalid Reports inspected, 1 report did not include annotations indicating how the errors were corrected.</p> <p><u>DFAS Pensacola</u></p> <p>Of the 45 Personnel Interface Invalid Reports selected for review, 1 report could not be located. Of the 44 Personnel Interface Invalid Reports inspected, 25 reports were annotated; however, sufficient detail did not exist to determine whether all errors within the report were resolved.</p> <p>In addition, 19 of the 44 Personnel Interface Invalid Reports inspected were annotated in Microsoft Word, but did not include the annotator's signature or date of annotation.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p><u>DFAS Charleston</u></p> <p>Personnel Interface Invalid Reports were neither annotated, nor available for review July 1, 2005, through February 13, 2006.</p> <p>Of the 45 Personnel Interface Invalid Reports selected for review, 3 reports could not be provided. None of the 42 Personnel Interface Invalid Reports inspected included a signature, date, and annotations indicating how the errors were corrected.</p>
7	Controls provide reasonable assurance that fiscal year-end, leave year-end, and calendar year-end processing occurs in accordance with established Government-wide and agency guidelines.	Policies and procedures are documented to describe how fiscal year-end, leave year-end, and calendar year-end processing occurs in accordance with established Government-wide and agency guidelines.	Inquired with appropriate personnel and read 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 established Government-wide and agency guidelines.	No relevant exceptions noted.
		Payroll withholding table data are periodically reviewed by supervisors for compliance with statutory requirements.	Inspected payroll withholding table data updates to confirm they are periodically updated by supervisory personnel for compliance with statutory requirements.	No relevant exceptions noted.
		The detailed "592" payroll reconciliation shows that 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 reconciled items	Inquired with appropriate personnel and examined a sample of 26 "592" reconciliations for each database to confirm the following conditions exist.  1) The detailed payroll reconciliation shows that only pertinent data describing the payroll (including total	<p><u>DFAS Pensacola</u></p> <p>Of the 26 "592" reconciliation reports inspected, 1 report did not include a preparer's signature and date. In addition, the Withholdings for Benefits report did not have a Certifying Officer's signature and date. However, DFAS Denver</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		<p>are investigated and cleared on a timely basis by supervisory personnel prior to disbursement.</p>	<p>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.</p> <p>2) Each “592” reconciliation is approved by management prior to disbursement.</p> <p>3) Reconciled items are investigated and cleared on a timely basis by supervisory personnel prior to disbursement.</p>	<p>maintained a signed copy of the “592” reconciliation report that they processed during contingency operations on behalf of DFAS Pensacola.</p> <p><u>DFAS Denver</u></p> <p>No relevant exceptions noted.</p> <p><u>DFAS Charleston</u></p> <p>No relevant exceptions noted.</p>
		<p>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; reviews output products for general acceptability; and reconciles control information to determine completeness of processing.</p>	<p>Inquired with appropriate personnel and inspected the schedules used by the data processing group to confirm that they:</p> <p>1) have 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;</p> <p>2) review output products for general acceptability;</p> <p>3) reconcile control information to determine completeness of processing.</p>	<p>No relevant exceptions noted.</p>
		<p>Users review the Personnel Interface Invalid Reports for data accuracy, validity, and completeness.</p>	<p>Inquired with appropriate personnel and inspected a random sample of 45 Personnel Interface Invalid Reports that users review for output to confirm that the reports are reviewed for data accuracy, validity, and completeness.</p> <p>Selected a random sample of 45 Personnel Interface Invalid Reports for the OMA pay database. In</p>	<p><u>DFAS Denver</u></p> <p><u>OMA Pay Database</u></p> <p>Of the 45 Personnel Interface Invalid Reports inspected, 3 reports did not include a date indicating when actions to correct the errors had been completed. In addition, 35 of the 45 Personnel Interface</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			<p>addition, the ZPA pay database only processed data for two pay periods, therefore, we reviewed all 16 Personnel Interface Invalid Reports during that period at DFAS Denver. As a result, 61 Personnel Interface Invalid Reports were selected for review at DFAS Denver.</p> <p>Selected a random sample of 45 Personnel Interface Invalid Reports beginning on February 14, 2006, at DFAS Charleston.</p>	<p>Invalid Reports inspected did not include annotations indicating how the errors were corrected.</p> <p><u>ZPA Pay Database</u></p> <p>Of the 16 Personnel Interface Invalid Reports inspected, 1 report did not include annotations indicating how the errors were corrected.</p> <p><u>DFAS Pensacola</u></p> <p>Of the 45 Personnel Interface Invalid Reports selected for review, 1 report could not be located. Of the 44 Personnel Interface Invalid Reports inspected, 25 reports were annotated; however, sufficient detail did not exist to determine whether all errors within the report were resolved.</p> <p>In addition, 19 of the 44 Personnel Interface Invalid Reports inspected were annotated in Microsoft Word, but did not include the annotator's signature or date of annotation.</p> <p><u>DFAS Charleston</u></p> <p>Personnel Interface Invalid Reports were neither annotated, nor available for review July 1, 2005, through February 13, 2006.</p> <p>Of the 45 Personnel Interface Invalid Reports selected for review, 3 reports could not be provided. None of the 42 Personnel Interface Invalid Reports inspected included a signature, date, and annotations indicating how the errors were corrected.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
8	Controls provide reasonable assurance that current- or prior-period adjustments to employee's pay, including employee debt, tax deduction, or deductions not taken, are reported, reconciled, and approved.	Policies and procedures are documented to describe how current- or prior-period adjustments to employee's pay, including employee debt, tax deductions, or deductions not taken, are reported, reconciled, and approved.	Inquired with appropriate personnel and read policies and procedures to confirm that current- or prior-period adjustments to employee's pay, including employee debt, tax deductions, or deductions not taken, are reported, reconciled, and approved.	No relevant exceptions noted.
		The detailed "592" payroll reconciliation shows that 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 reconciled items are investigated and cleared on a timely basis by supervisory personnel prior to disbursement.	<p>Inquired with appropriate personnel and examined a sample of 26 "592" reconciliations for each database to confirm that the following conditions exist.</p> <ol style="list-style-type: none"> <li>1) The detailed payroll reconciliation shows that 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.</li> <li>2) Each "592" reconciliation is approved by management prior to disbursement.</li> <li>3) Reconciled items are investigated and cleared on a timely basis by supervisory personnel prior to disbursement.</li> </ol>	<p><u>DFAS Pensacola</u> Of the 26 "592" reconciliation reports inspected, 1 report did not include a preparer's signature and date. In addition, the Withholdings for Benefits report did not have a Certifying Officer's signature and date. However, DFAS Denver maintained a signed copy of the "592" reconciliation report that they processed during contingency operations on behalf of DFAS Pensacola.</p> <p><u>DFAS Denver</u> No relevant exceptions noted.</p> <p><u>DFAS Charleston</u> No relevant exceptions noted.</p>
		OLQs and summary reports (including the Master Employee Add/Change/Delete Report) are periodically reviewed by supervisory personnel to determine if the master files remain accurate and pertinent.	Inquired with appropriate personnel and inspected OLQs and summary reports to confirm that master files are periodically reviewed by supervisory personnel.	No relevant exceptions noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		<p>The ability to view, modify, or transfer information contained in the payroll master files is restricted to authorized personnel.</p>	<p>Inquired with appropriate personnel and inspected a random sample of 45 access forms to confirm that the master file is restricted to authorized personnel.</p>	<p><u>DFAS Denver</u>  <u>Payroll Office Users</u>  Of the 12 SAAR forms selected for review, 1 form could not be located.</p> <p><u>Non-Payroll Office Users</u>  Of the 15 SAAR forms inspected, 1 form did not include the completion date of the initial computer-based security training. In addition, 1 of the 15 SAAR forms inspected did not include a supervisor's signature.</p> <p>The ZPA database included 42 users with supervisory-level access.</p> <p><u>DFAS Pensacola</u>  <u>Payroll Office Users</u>  Of the nine SAAR forms selected for review, one form could not be located. Of the eight SAAR forms inspected, two forms did not include the completion date of the initial computer-based security training.</p> <p><u>Non-Payroll Office Users</u>  Of the 26 SAAR forms selected for review, 4 forms could not be located. Of the 22 SAAR forms inspected, 3 forms did not include the completion date of the initial computer-based security training. In addition, 2 of the 22 SAAR forms inspected did not include the supervisor's signature.</p>



No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p><u>DFAS Charleston</u>  <u>Payroll Office Users</u>  Of the 24 SAAR forms selected for review, 1 form could not be located. Of the 23 SAAR forms inspected, 1 form did not match the level of authorized access actually granted.</p> <p>The Charleston payroll office had 133 DCPS users with access to update time and attendance and Master Employee data.</p> <p><u>Non-Payroll Office Users</u>  No relevant exceptions noted.</p>
		<p>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 management.</p>	<p>Inquired with appropriate personnel and inspected a random sample of 45 Remedy tickets to confirm that:</p> <ol style="list-style-type: none"> <li>1) tickets are pre-numbered,</li> <li>2) the sequence is accounted for so that the forms are accounted for timely,</li> <li>3) access to the source documents is controlled,</li> <li>4) key source documents require signatures from supervisory personnel, and</li> <li>5) tickets are completed within the required time frame.</li> </ol>	<p><u>DFAS Denver</u>  Of the 45 Remedy tickets inspected, 2 tickets were not completed within the required 3-10 day time frame.</p> <p><u>DFAS Pensacola</u>  Of the 45 Remedy tickets inspected, 3 tickets were not completed within the required 3-10 day time frame.</p> <p><u>DFAS-Charleston</u>  Of the 45 Remedy tickets inspected, 6 tickets were not completed within the required 3-10 day time frame.</p> <p><u>All Payroll Offices</u>  Remedy tickets were not sequentially numbered. Remedy tickets used for testing purposes were deleted. Documentation was not maintained for these tickets.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
9	All application users are appropriately identified and authenticated. Access to the application and output is restricted to authorized users for authorized purposes.	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.	Inquired with appropriate personnel and read 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.	No relevant exceptions noted.
		Online access logs are maintained by the SMO and the logs are reviewed regularly for unauthorized access attempts.	Inquired with appropriate personnel and inspected access logs and e-mails for unauthorized access attempts to confirm that logs are maintained by the SMO and the logs are reviewed regularly for unauthorized access attempts.	No relevant exceptions noted.
		<p>Each operator is required to complete a SAAR form before being granted access to the system.</p> <p>The ability to view, modify, or transfer information contained in the payroll master files is restricted to authorized personnel.</p>	Inquired with appropriate personnel and inspected a random sample of 45 user authorization forms to confirm that each operator is authorized before being granted access to the system and that the DCPS master file and output is restricted to authorized users for authorized purposes.	<p><u>DFAS Denver</u> <u>Payroll Office Users</u> Of the 12 SAAR forms selected for review, 1 form could not be located.</p> <p><u>Non-Payroll Office Users</u> Of the 15 SAAR forms inspected, 1 form did not include the completion date of the initial computer-based security training. In addition, 1 of the 15 SAAR forms inspected did not include a supervisor's signature.</p> <p>The ZPA database included 42 users with supervisory-level access.</p> <p><u>DFAS Pensacola</u> <u>Payroll Office Users</u> Of the nine SAAR forms selected for review, one form could not be located. Of the eight SAAR forms inspected, two forms did not</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>include the completion date of the initial computer-based security training.</p> <p><u>Non-Payroll Office Users</u></p> <p>Of the 26 SAAR forms selected for review, 4 forms could not be located. Of the 22 SAAR forms inspected, 3 forms did not include the completion date of the initial computer-based security training. In addition, 2 of the 22 SAAR forms inspected did not include the supervisor's signature.</p> <p><u>DFAS Charleston</u></p> <p><u>Payroll Office Users</u></p> <p>Of the 24 SAAR forms selected for review, 1 form could not be located. Of the 23 SAAR forms inspected, 1 form did not match the level of authorized access actually granted.</p> <p>The Charleston payroll office had 133 DCPS users with access to update time and attendance and Master Employee data.</p> <p><u>Non-Payroll Office Users</u></p> <p>No relevant exceptions noted.</p>
		<p>Departmental managers periodically review listings (including the Personnel/Payroll Reconciliation and Control of Hours Report) of current employees within their departments and notify the personnel department of necessary changes.</p>	<p>Inquired with appropriate personnel and inspected the Personnel/Payroll Reconciliation and Control of Hours reports to confirm that they are sent to management for review of employee listings and notification to personnel department of changes.</p>	<p>No relevant exceptions noted.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
10	Controls provide reasonable assurance that data transmissions in DCPS from user organizations are authorized, complete, accurate, and secure.	Policies and procedures are documented to describe how data transmissions in DCPS from organizations are authorized, complete, accurate, and secure.	Inquired with appropriate personnel and read policies and procedures to confirm that data transmissions between DCPS and user organizations are authorized, complete, accurate, and secure.	No relevant exceptions noted.
		Compliance with the payroll disbursement processing schedule is monitored by management.	Inquired with appropriate personnel, inspected pay processing schedules, and observed the payroll disbursement process to confirm the monitoring of payroll disbursement processing schedule by management.	No relevant exceptions noted.
		<p>Each operator is required to complete a SAAR form before being granted access to the system.</p> <p>User profiles limit what transactions data entry personnel can input.</p>	<p>Inquired with appropriate personnel and inspected a random sample of 45 user authorization forms to confirm that each operator is required to have an authorization form before being granted access to the system and user profiles limit what transactions data entry personnel can input.</p>	<p><u>DFAS Denver</u></p> <p><u>Payroll Office Users</u></p> <p>Of the 12 SAAR forms selected for review, 1 form could not be located.</p> <p><u>Non-Payroll Office Users</u></p> <p>Of the 15 SAAR forms inspected, 1 form did not include the completion date of the initial computer-based security training. In addition, 1 of the 15 SAAR forms inspected did not include a supervisor's signature.</p> <p>The ZPA database included 42 users with supervisory-level access.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p><u>DFAS Pensacola</u></p> <p><u>Payroll Office Users</u></p> <p>Of the nine SAAR forms selected for review, one form could not be located. Of the eight SAAR forms inspected, two forms did not include the completion date of the initial computer-based security training.</p> <p><u>Non-Payroll Office Users</u></p> <p>Of the 26 SAAR forms selected for review, 4 forms could not be located. Of the 22 SAAR forms inspected, 3 forms did not include the completion date of the initial computer-based security training. In addition, 2 of the 22 SAAR forms inspected did not include the supervisor's signature.</p> <p><u>DFAS Charleston</u></p> <p><u>Payroll Office Users</u></p> <p>Of the 24 SAAR forms selected for review, 1 form could not be located. Of the 23 SAAR forms inspected, 1 form did not match the level of authorized access actually granted.</p> <p>The Charleston payroll office had 133 DCPS users with access to update time and attendance and Master Employee data.</p> <p><u>Non-Payroll Office Users</u></p> <p>No relevant exceptions noted.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		Remote terminal connections are secured and are connected through Government-issued computers.	Inquired with appropriate personnel and observed remote terminal connections to confirm they are secured and are connected through Government computers.	No relevant exceptions noted.
		Data entry terminals are connected to the system only during specified periods of the day, which corresponds with the business hours of the data entry personnel.	Inquired with appropriate personnel and observed after-hours processes to confirm terminals are not authorized to be connected after business hours.	No relevant exceptions noted.
		User identification and passwords are required to gain access to the DCPS application.	Inquired with appropriate personnel and observed the DCPS log-in screen to confirm that user identification and passwords are required to gain access to the DCPS application.	No relevant exceptions noted.
		Online access logs are maintained by the SMO and the logs are reviewed regularly for unauthorized access attempts.	Inquired with appropriate personnel and inspected access logs and e-mails for unauthorized access attempts to confirm that logs are maintained by the SMO and the logs are reviewed regularly for unauthorized access attempts.	No relevant exceptions noted.
		Each terminal automatically disconnects from the system when not used after a specified period of time.	Inquired with appropriate personnel and observed system inactivity to confirm that each terminal automatically disconnects from the system when not used within 15 minutes.	No relevant exceptions noted.
		When terminals are not in use, terminal rooms are locked or the terminals are secured.	Inquired with appropriate personnel and observed the facility to confirm that when terminals are not in use, terminal rooms are locked or the terminals were secured.	No relevant exceptions noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
11	Controls are reasonable to ensure that transmissions from interfacing systems are subjected to the payroll system edits, validations, and error-correction procedures.	Policies and procedures are documented to describe how transactions from interfacing systems are subjected to the payroll system edits, validations, and error-correction procedures.	Inquired with appropriate personnel and read policies and procedures to confirm that transactions from interfacing systems are subjected to the payroll system edits, validations, and error-correction procedures.	No relevant exceptions noted.
		A control group is responsible for controlling and monitoring rejected transmissions included on the Personnel Interface Invalid Report.	<p>Inquired with appropriate personnel and inspected a random sample of 45 Personnel Interface Invalid Report to confirm that the report is used for controlling and monitoring rejected transactions.</p> <p>Selected a random sample of 45 Personnel Interface Invalid Reports for the OMA pay database. In addition, the ZPA pay database only processed data for two pay periods, therefore, we reviewed all 16 Personnel Interface Invalid Reports during that period at DFAS Denver. As a result, 61 Personnel Interface Invalid Reports were selected for review at DFAS Denver.</p> <p>Selected a random sample of 45 Personnel Interface Invalid Reports beginning on February 14, 2006, at DFAS Charleston.</p>	<p><u>DFAS Denver</u> <u>OMA Pay Database</u></p> <p>Of the 45 Personnel Interface Invalid Reports inspected, 3 reports did not include a date indicating when actions to correct the errors had been completed. In addition, 35 of the 45 Personnel Interface Invalid Reports inspected did not include annotations indicating how the errors were corrected.</p> <p><u>ZPA Pay Database</u></p> <p>Of the 16 Personnel Interface Invalid Reports inspected, 1 report did not include annotations indicating how the errors were corrected.</p> <p><u>DFAS Pensacola</u></p> <p>Of the 45 Personnel Interface Invalid Reports selected for review, 1 report could not be located. Of the 44 Personnel Interface Invalid Reports inspected, 25 reports were annotated; however, sufficient detail did not exist to determine whether all errors within the report were resolved.</p>

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<p>In addition, 19 of the 44 Personnel Interface Invalid Reports inspected were annotated in Microsoft Word, but did not include the annotator's signature or date of annotation.</p> <p><u>DFAS Charleston</u></p> <p>Personnel Interface Invalid Reports were neither annotated, nor available for review July 1, 2005, through February 13, 2006.</p> <p>Of the 45 Personnel Interface Invalid Reports selected for review, 3 reports could not be provided. None of the 42 Personnel Interface Invalid Reports inspected included a signature, date, and annotations indicating how the errors were corrected.</p>
		<p>The data processing control group maintains a schedule by application that shows when outputs should be completed, when they need to be distributed, who the recipients are, and the number of copies needed; reviews output products for general acceptability; and reconciles control information to determine completeness of processing.</p>	<p>Inquired with appropriate personnel and inspected schedules used by the data processing group to confirm that they:</p> <ol style="list-style-type: none"> <li>1) maintain a schedule by application that shows when outputs need to be completed, when they need to be distributed, who the recipients are, and the number of copies needed;</li> <li>2) review output products for general acceptability; and</li> <li>3) reconcile control information to determine completeness of processing.</li> </ol>	<p>No relevant exceptions noted.</p>
		<p>The system provides an audit trail of all transactions processed, transaction errors, error descriptions, and error correction procedures. Inquire</p>	<p>Inquired with appropriate personnel and inspected audit trails to confirm that payroll technicians captured, reported, investigated, and corrected</p>	<p>No relevant exceptions noted.</p>



No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		whether audit trails are reviewed by supervisory personnel. Inquire whether payroll technicians capture, report, investigate, and correct erroneous data.	erroneous transactions and those transactions were reviewed by supervisory personnel.	
		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 re-entered.	Inquired with appropriate personnel and inspected interface files to confirm that record counts match control totals in the footer and out-of-balance conditions were reported, corrected, and re-entered.	No relevant exceptions noted.
		Batch transactions without pre-assigned serial numbers are automatically assigned a unique sequence number which is used by the computer for ensuring that all transactions are processed.	Observed the batch process to confirm that transactions without pre-assigned serial numbers were automatically assigned a unique sequence number.	No relevant exceptions noted.
12	Controls provide reasonable assurance that personnel payroll records and other sensitive information is maintained and disposed of in accordance with Government-wide and agency specific guidelines.	Policies and procedures are documented to describe how 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 read 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.	No relevant exceptions noted.
All documents and storage media are stored in physically and environmentally secure containers.		Inquired with appropriate personnel and observed storage processes to confirm documents and storage media are properly stored in environmentally secure containers.	No relevant exceptions noted.	
All visitors to the payroll offices must sign-in and out with the authorized security personnel.		Inquired with appropriate personnel and inspected visitor logs at the payroll offices to confirm that visitors signed in and out with the authorized security personnel.	No relevant exceptions noted.	

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		All terminals and payroll records are located in physically secured locations.	Inquired with appropriate personnel and observed the terminal rooms to confirm the rooms are physically secure.	No relevant exceptions noted.
		Users dispose of personnel and payroll records in accordance with Government-wide and agency-specific guidelines.	Inquired with appropriate personnel and observed destruction bins to confirm that payroll records are disposed of in accordance with Government-wide and agency-specific guidelines.	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
	<i>Enterprise-Wide Security Program Planning</i>			
1	Risks are periodically assessed.	<p><u>DECC SMC Mechanicsburg and DFAS TSOPE</u></p> <p>DoD and DFAS policy direct an annual IA review. Review appropriate documentation to ensure that these processes are completed.</p>	<p><u>DISA</u></p> <p>Inquired of the Information System Security Officer and related security personnel how often the risk assessment process occurs.</p> <p>Inspected the latest Risk Assessment that was included with the SSAA to confirm that risks are periodically assessed.</p> <p>Inquired of appropriate personnel about the SRR process and determined how often SRRs occur and if deficiencies and corrective actions are tracked.</p> <p>Selected a sample of SRRs performed and inspected the Vulnerability Management System (VMS) reports to confirm that findings identified by the SRR process have been addressed.</p> <p>Requested the following documents: Facility Risk Assessment, System Administrator (SA) Report, DCPS Local Exemptions, DCPS Specific Audit Server Findings (SRR Report), and the Automated Information System Connectivity Process.</p> <p><u>DFAS</u></p> <p>Inquired of the Information Systems Security Officer and related security personnel how often the risk assessment process occurs.</p>	<p><u>DISA FSO</u></p> <p>An SRR was not completed within the last 3 years for the LPAR where the DCPS application was housed.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			<p>Inspected the lasted Risk Assessment that was included with the SSAA to confirm that risks are periodically assessed.</p> <p>Determined what other internal processes (if any) DFAS performs to assess risks</p>	
2	A security plan is documented, approved, and kept current.	<p><u>DFAS TSOPE</u></p> <p>DoD and DFAS policy direct an annual IA review. Review appropriate documentation to ensure that these processes are accomplished.</p>	<p><u>DFAS</u></p> <p>Inspected the DCPS SSAA to confirm it has been documented, approved by management, and kept current.</p> <p>Inspected DCPS Systems Security Policy, Security Requirements, and Certification Test and Evaluation Plan and Procedures to confirm that each has been updated.</p>	No relevant exceptions noted.
3	A security management structure has been established, and information security responsibilities are assigned, clearly defined, and in place for all personnel.	<p><u>DECC SMC Mechanicsburg</u></p> <p>The DECC SMC Mechanicsburg SSAA includes Appendix J, "System Rules of Behavior," which describes IA operations of the DoD information system and clearly delineates IA responsibilities and expected behaviors of all personnel.</p>	<p><u>DISA</u></p> <p>Confirmed through inquiry that a management structure had been established.</p> <p>Obtained and inspected the security management organization chart.</p> <p>Requested one position description for each function listed on the organization chart to confirm that all positions were established in writing.</p> <p>Inspected the SSAA for the security management structure. Confirmed that each position function is outlined in the SSAA.</p> <p>Inspected the SSAA for security management responsibilities. Confirmed that each position is outlined in the SSAA and is filled and that personnel understand their responsibilities.</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			Inspected signed rules of behavior statements for the DISA personnel with access to DCPS and the underlying operating system.	
4	Owners and users are aware of security policies.	<p><u>DECC SMC Mechanicsburg</u></p> <p>Ongoing security awareness curriculum includes: New Employee Security Briefing; Annual Security Briefing; IA Awareness Training; Courier Briefing; SF 312 Non-Disclosure Briefing; Antiterrorism Force Protection Briefing; and SA Training.</p> <p>A Security page on Command Intranet site has been established.</p> <p><u>DFAS TSOPE</u></p> <p>Ongoing security awareness programs that include initial training and periodic refresher training have been established.</p>	<p><u>DISA</u></p> <p>Inspected the Security Awareness Training materials.</p> <p>Selected a random sample of employees and inspected their training files to confirm the completion of necessary security training and that training has been signed off by a supervisor.</p> <p>Inspected the training sign-in sheets to confirm that employees had attended annual training.</p> <p>Obtained evidence that management has active security awareness programs in place (that is electronic mail files or other policy distribution mechanisms) that proactively emphasized the security policies to data owners and users.</p> <p><u>DFAS</u></p> <p>Inspected the Security Awareness Training materials.</p> <p>Obtained a list of employees who have access to DCPS.</p> <p>Selected a random sample of employees who have DCPS access and inspected their training files to confirm the completion of necessary security training and that training has been signed off by a supervisor.</p> <p>Inspected the training sign-in sheets to confirm that employees had attended annual training.</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			<p>Obtained evidence that management has active security awareness programs in place (that is electronic mail files or other policy distribution mechanisms) that proactively emphasized the security policies to data owners and users.</p>	
5	<p>An incident response capability has been implemented.</p>	<p><u>DECC SMC Mechanicsburg</u> DISA Policy Letter 05-04, "Computer Security Incident Handling and Reporting," May 4, 2005, has been implemented.</p>	<p><u>DISA</u> Confirmed through inspection that the incident plan detailed in the SSAA has been implemented.  Obtained a list of all incidents that occurred during the audit period. Selected a random sample of incidents to confirm that the incident response plan was being followed.</p>	<p>No relevant exceptions noted.</p>
6	<p>Hiring, transfer, termination, and performance policies address security.</p>	<p><u>DECC SMC Mechanicsburg</u> Personnel and Industrial Security Program(s) are implemented in accordance with DoD Directive 5200.2-R, "DoD Personnel Security Program," April 9, 1999, DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003, and the Computing Services Security Handbook, February 27, 2006.</p>	<p><u>DISA</u> Inspected the hiring, transfer, termination, and performance policies to confirm they are documented and address security.  Confirmed through inquiry that debriefs were conducted when employees were terminated and that a DISA Form 70 is used to note the collection of DISA property.  Confirmed through observation that an e-mail was sent to the SA to request that system access be removed for a terminated employee.</p>	<p><u>DISA DECC SMC Mechanicsburg</u> Of the 23 Personnel Out-Processing Forms reviewed, 1 form did not include a signature and date indicating that access to the mainframe was removed.  Of the 23 Personnel Out-Processing Forms reviewed, 1 form included appropriate approval to remove access to the mainframe; however, the form was not dated.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
				Of the 23 Personnel Out-Processing Forms reviewed, 2 forms indicated mainframe system access was removed after the employees left DECC SMC Mechanicsburg. As a mitigating circumstance, all the users listed on these forms did not have access to DCPS.
7	A training program is implemented to provide assurance that employees have adequate training and expertise.	<p><u>DECC SMC Mechanicsburg</u> A robust Security Awareness curriculum that includes: New Employee Security Briefing, Annual Security Briefing, information assurance Awareness Training, Courier Briefing, SF 312 Non-Disclosure Briefing, Antiterrorism Force Protection Briefing, and SA training has been implemented.</p> <p><u>DFAS TSOPE</u> Ongoing security awareness programs that include initial training and periodic refresher training is implemented.</p> <p>Additionally, the DCPS SSAA includes Appendix J, "System Rules of Behavior," which describes the IA operations of the DoD information system and clearly delineates IA responsibilities and expected behavior of all personnel.</p>	<p><u>DISA</u> Confirmed through inquiry that a training program had been established. Requested documentation to confirm the existence of this training program. If training is conducted in-house, inspected training materials to confirm that they provided personnel with adequate training and expertise. Selected a random sample of training records for employees who had access to DCPS. Inspected the training records to ensure functional job training was occurring.</p> <p><u>DFAS</u> Confirmed through inquiry that a training program has been established. Requested documentation to confirm the existence of this training program. If training is conducted in-house inspected training materials to confirm that they provided personnel with adequate training and expertise and that they are up to date.</p>	<p><u>DECC SMC Mechanicsburg</u> A structured functional training program had not been established at DECC SMC Mechanicsburg for all Government personnel and contractors with access to the DCPS mainframe. In addition, a process did not exist to independently verify that personnel had completed training and submitted training completion certificates. However, DECC SMC Mechanicsburg has a process for users to obtain training.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			Selected a random sample of employees who had access to DCPS. Inspected the training records to ensure that functional job training was occurring.	
8	Management periodically assesses the appropriateness of security policies and compliance with them.	<u>DECC SMC Mechanicsburg</u> The Director's Policy Letters and standard operating procedures are reviewed and updated. An SRR is conducted at least once every 3 years.	<u>DISA</u> Interviewed the Security Manager to obtain an understanding of how management assessed appropriateness of and compliance with security policies.  Inspected the DCPS Security Requirements and Information Systems Security Policy Certification Test and Evaluation Procedures to confirm that an annual IA review was conducted and that comprehensive vulnerability management was in place.	<u>DISA FSO</u> An SRR was not completed within the last 3 years for the LPAR where the DCPS application was housed.
9	Management ensures that corrective actions are effectively implemented.	<u>DECC SMC Mechanicsburg</u> The VMS is used to track findings identified during the SRR process. DECC SMC Mechanicsburg management is responsible for tracking and closing all findings that resulted from the SRR process.  <u>DFAS TSOPE</u> Management tracks prior audit reports and confirms that observations are corrected in a timely manner.	<u>DISA</u> Inquired of appropriate personnel about the SRR process to confirm that corrective actions are effectively implemented for identified SRR findings.  Selected a random sample of SRRs and inspected the VMS reports to confirm that findings identified by the SRR process have been addressed.  Requested prior audit reports or reviews and determined if remediation has occurred for the findings and recommendations contained within those reports.	<u>DISA FSO</u> An SRR was not completed within the last 3 years for the LPAR where the DCPS application was housed.



No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			<p><u>DFAS</u></p> <p>Requested prior audit reports or reviews and determined if remediation has occurred for the findings and recommendations presented within those reports.</p>	
10	<p>A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place.</p>	<p><u>DECC SMC Mechanicsburg</u></p> <p>Vulnerabilities are tracked in the VMS database. Prior to connecting to the network, the SA must run a VS08 report detailing IA Vulnerability Management notices for the asset's operating system. All IA Vulnerability Management notices must be mitigated, and applicable patches loaded prior to connecting the asset to the network. Once all checklists have been applied from the STIG and the vulnerability alerts have been installed, a SRR and an information security scan will be conducted on the operating system. Security assessments that require a scan will use the Internet Security Scanner and the FSO Full Scan Policy. The scan will be conducted using a direct connection from the system running Internet Security Scanner to the system being assessed or the site is authorized to connect the asset to an isolated network during the Internet security scan. Each site will place their self-assessment in the Security Readiness Review Database. If the systems have a database, web server, or any other software that has a STIG, they must go through a FSO SRR and the results put in the self-assessment of the SRR database.</p>	<p><u>DISA</u></p> <p>Inspected the vulnerability management policy and documentation to confirm that the process includes systematic identification and mitigation of software and hardware vulnerabilities.</p> <p>Inspected a random sample of vulnerability assessments to confirm that vulnerabilities were identified and resolved.</p> <p>Obtained the VMS reports for the audit period for DCPS and confirmed vulnerabilities were tracked and resolved in a timely manner.</p>	<p><u>DISA FSO</u></p> <p>An SRR was not completed within the last 3 years for the LPAR where the DCPS application was housed.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
11	Changes to the DoD information systems are assessed for IA and accreditation impact prior to implementation.	<u>DFAS TSOPE</u> All changes made are captured in the Change Management Information System. Information for each change record includes the requested time and date of implementation, the action to occur, and justification of the action.	<u>DFAS</u> Inspected evidence that management assesses if a change is IA compliant and if the change impacts accreditation before moving the change into the production environment.	<u>DFAS TSOPE</u> The configuration management process required only program code changes to be assessed and evaluated for IA impact. Of the 45 changes reviewed, 24 changes impacted program code. Of the 24 changes impacting program code, 5 changes were not assessed and evaluated by the IA Officer for IA impact.
12	A DoD reference document constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA and IA-enabled information technology (IT) products.	<u>DECC SMC Mechanicsburg</u> DISA has developed and requires compliance with the STIGs appropriate to the operating system, application, or hardware.	<u>DISA</u> Inspected the DISA Database STIG, DISA UNIX STIG, and DISA Instruction Information Systems Security Program 630-230-19 to confirm that those policies constitute the primary source configuration or implementation guidance for the deployment of newly acquired IA and IA-enabled products.	No relevant exceptions noted.
	<i>Access Controls</i>			
13	Application owners have determined classification of resources, and related criteria for access administration have been established.	<u>DFAS TSOPE</u> Management has classified DCPS according to appropriate MAC level standards.	<u>DFAS</u> Inspected the DCPS SSAA and confirmed that a MAC level had been assigned to DCPS.  Inquired with data owners and confirmed that a MAC level had been assigned to DCPS.	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
14	Resource owners have a process in place to identify users and all user access is authorized.	<p><u>DFAS TSOPE</u></p> <p>The SAAR form is used to identify authorized users and control their access to DCPS.</p>	<p><u>DFAS</u></p> <p>Requested a complete DCPS user list.</p> <p>Selected a random sample of 45 user forms from the list. Inspected the user SAAR forms for existence and management's approval.</p> <p>Observed the application to confirm that users possessed valid user identification and a password to gain access to the system.</p> <p>Interviewed the system owner (DFAS) and inspected supporting documentation to confirm that unauthorized access to the system is removed in a timely manner.</p> <p>Interviewed Security Managers and confirmed that Security Managers provided appropriate supporting documentation.</p> <p>Obtained a representative sample of user 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 Human Resources Department. Selected a representative sample of terminated employees and confirmed that system access had been promptly terminated.</p>	No relevant exceptions noted.
15	Emergency and temporary access authorization is controlled.	<p><u>DECC SMC Mechanicsburg</u></p> <p>Emergency and temporary access authorization is controlled in accordance with DoD 5200.1-R, DoD 5200.2-R, DoD Directive 8500.1, DoD Instruction 8500.2, and the Computing Services Security Handbook.</p>	<p><u>DISA</u></p> <p>Inspected the emergency and temporary access policy.</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			<p>Selected a random sample of emergency and temporary access requests to confirm that:</p> <ul style="list-style-type: none"> <li>• the authorization was approved and that access was closed in a timely manner.</li> <li>• the emergency and temporary access list was periodically reviewed.</li> <li>• all temporary access authorizations were established for least privileged need-to-know access.</li> </ul>	
16	Owners determine disposition and sharing of data.	<p><u>DFAS TSOPE</u></p> <p>Policies and procedures that govern the sharing of data are documented in the SSAA.</p>	<p><u>DFAS</u></p> <p>Inspected documents authorizing file sharing and file sharing agreements and confirmed that the owners approve the sharing of data. In many cases those documents are called memorandums of agreement or Service-Level agreements.</p> <p>Inspected the DCPS SSAA and confirmed that a MAC level had been assigned to DCPS.</p> <p>Inquired with data owners (DFAS) and confirmed that a MAC level had been assigned to DCPS.</p>	<p><u>DFAS SMO</u></p> <p>Of the 109 systems that interface with DCPS, 79 did not have a documented memorandum of agreement in place.</p>
17	Adequate physical security controls have been implemented that are commensurate with the risks of physical damage or access.	<p><u>DECC SMC Mechanicsburg</u></p> <p>All DISA facilities at DECC SMC Mechanicsburg are locked at all times. Access is restricted using proximity cards with personal identification number technology, which are controlled and issued by the Security Manager.</p>	<p><u>DISA</u></p> <p>Observed and documented the physical safeguards in place and confirmed that safeguards are established to mitigate the risk of physical damage or access.</p> <p>Observed that facility penetration testing processes are in place to include periodic, unannounced attempts to penetrate key computing facilities. In addition, we observed that every</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		<p>The Naval Inventory Control Point conducts periodic, unannounced penetration testing to confirm that physical security is adequate.</p> <p>The DECC SMC Mechanicsburg SSAA requires the Security Office to perform physical security inspections.</p>	<p>physical access point that displays sensitive information or unclassified information that had not been cleared for release was controlled during business hours and guarded or locked during non-business hours.</p>	
18	Visitors are controlled.	<p><u>DECC SMC Mechanicsburg</u></p> <p>Visitor access is controlled in accordance with DoD 5200.2-R, DoD 5200.1-R, and the Computing Services Security Handbook. DECC SMC Mechanicsburg uses access control databases, proximity cards with personal identification number technology, vetted badge exchange, visitor logs, and visit authorization Requests.</p> <p><u>DFAS TSOPE</u></p> <p>All visitors must sign in and sign out with the guard on duty.</p> <p>The DCPS SSAA requires all non-cleared personnel to be escorted at all times while inside the building.</p>	<p><u>DISA</u></p> <p>Inspected visitor access policies and procedures to confirm those policies are documented.</p> <p>Observed the visitor sign-in and sign-out process.</p> <p>Confirmed through inquiry that all visitors are escorted.</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><u>DFAS</u></p> <p>Inspected visitor access policies and procedures to confirm that those policies are documented.</p> <p>Observed the visitor check-in and check-out process.</p> <p>Confirmed through inquiry that all visitors are escorted.</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><u>DECC SMC Mechanicsburg</u></p> <p>Of the 45 daily visitor logs reviewed, 1 log did not include completed information for each visitor that entered DECC SMC Mechanicsburg that day. As a mitigating circumstance, the visitor was signed out by DECC SMC Mechanicsburg personnel, but the time the visitor left was not completed in the log.</p> <p><u>DFAS TSOPE</u></p> <p>Of the 45 daily visitor logs selected for review, 11 logs could not be located. Of the 34 logs reviewed, 12 logs did not include completed information for each visitor that entered DFAS TSOPE on those days. As a mitigating circumstance, the facility is protected by access-control locks and all visitors must be escorted by DFAS employees.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
19	Adequate logical access controls have been implemented at the application layer.	<p><u>DFAS TSOPE</u></p> <p>User identification and passwords are configured according to DoD standards.</p>	<p><u>DFAS</u></p> <p>Observed that each user account was assigned a security profile that restricted access by module, program, unit identification code, and hand receipt.</p> <p>Requested a complete DCPS user list. Selected a random sample of DCPS users from the list and inspected their SAAR forms to confirm that the forms existed and were approved by management.</p> <p>Inquired with DFAS personnel to confirm that users possessed valid user identification and a password to gain access to the system.</p> <p>Interviewed the system owner (DFAS) and inspected supporting documentation to confirm that unauthorized access to the system is removed in a timely manner.</p> <p>Interviewed Security Managers and confirmed that Security Managers provided appropriate supporting documentation.</p> <p>Confirmed through inquiry that profile changes are not recorded in activity logs. All profile changes are completed on the SAAR forms, and this form requires management's approval.</p> <p>Obtained a list of recently terminated employees from the Human Resources Department. Selected a representative sample of terminated employees and confirmed that system access had been promptly terminated.</p>	<p><u>DFAS TSOPE</u></p> <p>The current version of ACF2 allowed for password character complexity as required by DoD Instruction 8500.2. However, DCPS was not configured to use the complex characters and, therefore, was not in compliance with DoD Instruction 8500.2. As a mitigating circumstance, DCPS is still subject to password controls that included periodic changing and minimum character lengths.</p> <p>In addition, the password configuration requirements cannot be changed unless DFAS requests complex password configuration.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
20	<p>Passwords, tokens, or other devices are used to identify and authenticate users.</p>	<p><u>DECC SMC Mechanicsburg and DFAS TSOPE</u></p> <p>Multiple layers of access controls are used including: common access card and personal identification number, DCPS user identification and password, and a Regional Support Activity SecurID for Database Administration, Configuration Management, Security, and Technical Support.</p>	<p><u>DISA</u></p> <p>Confirmed through inquiry and observation that passwords are used to authenticate users.</p> <p>Inspected system parameters to ensure that the system requires user identification and a password.</p> <p>Inspected the Security Account Creation Guide to confirm that authentication devices were in compliance with DoD standards.</p> <p><u>DFAS</u></p> <p>Observed DCPS login procedures to confirm that users needed valid user identification and a password to gain access to the system.</p> <p>Inspected system parameters to ensure that the system requires user identification and a password.</p>	<p><u>DFAS TSOPE</u></p> <p>The current version of ACF2 allowed for password character complexity as required by DoD Instruction 8500.2. However, DCPS was not configured to use the complex characters and, therefore, was not in compliance with DoD Instruction 8500.2. As a mitigating circumstance, DCPS is still subject to password controls that included periodic changing and minimum character lengths.</p> <p>In addition, the password configuration requirements cannot be changed unless DFAS requests complex password configuration.</p>
21	<p>Access paths are identified as part of a risk analysis and documented in an access path diagram.</p>	<p><u>DECC SMC Mechanicsburg</u></p> <p>Access paths are identified as part of the DECC SMC Mechanicsburg enclave SSAA and documented in the network diagram within the SSAA.</p> <p>Firewalls and routers are used to restrict access within the network.</p>	<p><u>DISA</u></p> <p>Confirmed through inquiry that user management controls, firewalls, intrusion detection systems (IDS), and authentications were used to control network access.</p> <p>Obtained and inspected the network diagrams for DECC SMC Mechanicsburg to confirm that access paths were documented and monitored by IDSs.</p>	<p>No relevant exceptions noted.</p>
22	<p>Access is restricted to data files and software programs.</p>	<p><u>DECC SMC Mechanicsburg</u></p> <p>The System Support Office, a unit independent of DECC SMC Mechanicsburg operations, is responsible for maintaining the system</p>	<p><u>DISA</u></p> <p>Confirmed through inquiry and inspection of a list of the root access users for the DCPS servers that the access restrictions had been established</p>	<p><u>DECC SMC Mechanicsburg</u></p> <p>Of the 45 SAAR forms reviewed, 4 forms did not include justification for granting access to DCPS. In addition, 1</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		libraries. Access to system libraries is restricted to authorized individuals.	for data files and software programs. Inspected the access logs and inquired with management whether access logs were reviewed for unauthorized access and whether system libraries were managed and maintained to protect privileged programs. Inspected a random sample of SAAR forms to confirm that each form includes the user's justification for access, security clearance level, and approval from management.	of the 45 SAAR forms reviewed did not indicate the organization requesting access for the user.
23	Access settings have been implemented in accordance with the access authorizations established by the resource owners.	<p><u>DECC SMC Mechanicsburg</u> Access settings have been implemented in accordance with the access authorization established by signature authority of the resource owner on the SAAR form and in accordance with DoD Directive 8500.1, DoD Instruction 8500.2, and DISA STIGs.</p> <p><u>DFAS TSOPE</u> The Technical Support Office assigns security profiles to each user's identification based on need-to-know as demonstrated by an approved SAAR form. TSOPE Database Administrators also assign security profiles to development users through IDMS, which restricts access to program libraries and databases.</p>	<p><u>DISA</u> Inspected a random sample of 45 SAAR forms to confirm that each form includes the user's justification for access, security clearance level, and approval from management.</p> <p><u>DFAS</u> Observed that each user account was assigned a security profile that restricted access by module or program.</p>	<p><u>DECC SMC Mechanicsburg</u> Of the 45 SAAR forms reviewed, 4 forms did not include justification for granting access to DCPS. In addition, 1 of the 45 SAAR forms reviewed did not indicate the organization requesting access for the user.</p> <p><u>DFAS TSOPE</u> DFAS TSOPE Database Administrators had unrestricted access and made changes directly to payroll data recorded in IDMS by using a Data Manipulation Language Online tool. Although those changes were recorded in an audit log, TSOPE management did not review those logs regularly to determine whether the changes were appropriate and had been approved.</p> <p>In addition, three active user accounts on the IDMS user access list were identified; however, those accounts were not associated with personnel</p>



No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
				<p>who needed that type of access. Specifically, one account was for an individual no longer employed by DFAS TSOPE, one account was a duplicate account, and one account was for an individual that no longer required that level of access. However, as a mitigating circumstance, access to IDMS was controlled through the ACF2 utility. None of the three account holders had access to ACF2.</p> <p>DFAS TSOPE technical support personnel had unrestricted access to flat files that contain DCPS customer data sent for processing or DCPS files that contain payroll, bank account, and other personal information. The technical support personnel had the ability to edit data within flat files. As a mitigating circumstance, audit logs recorded the date, time, and user identification of the person accessing the flat files; however, the audit logs did not record the type of change that had been made.</p> <p>In addition, as part of the payroll process, file balancing would identify any changes to amounts within the flat files.</p>
24	Telecommunications controls are properly implemented in accordance with granted authorizations.	<u>DECC SMC Mechanicsburg</u> Remote access to the Internet is regulated by positive technical controls (including firewalls, routers, and proxy services and screened subnets, also called demilitarized zones [DMZ]), or	<u>DISA</u> Confirmed through inquiry and inspection of policy that telecommunications controls were implemented.	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		<p>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 SAs which require Secure Shell restrictions. Enterprise Security Manager is installed on some of these systems.</p>	<p>Observed the existence of intrusion detection telecommunication monitoring controls.</p> <p>Obtained firewall rules to document acceptable telecommunication protocols and compared them with policy to confirm compliance.</p>	
25	<p>Procedures are in place to clear sensitive information and software from computers, disks, and other equipment or media when they are disposed of or transferred for other use.</p>	<p><u>DECC SMC Mechanicsburg</u></p> <p>All documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released. A signature is required to certify the destruction of such media.</p>	<p><u>DISA</u></p> <p>Requested and inspected the Disposition of Unclassified DoD Computer Hard Drives policy and confirmed the policy was followed.</p> <p>Observed that media was stored in a secure room before the media was cleared or destroyed.</p> <p>Observed the procedures in place to clear or destroy equipment and media.</p>	<p>No relevant exceptions noted.</p>
26	<p>Audit trails are maintained in the application, operating system, and database.</p>	<p><u>DECC SMC Mechanicsburg and DFAS TSOPE</u></p> <p>A security audit trail that documents the identity of each person or device having access to a system, the time of that access, user activity, and any actions which attempt to change established security levels or privileges for the user is implemented for each system.</p>	<p><u>DISA</u></p> <p>Confirmed through inquiry that audit trails were maintained for the application and operating system.</p> <p>Inspected available audit trails and determined that the activities of users with root access were logged. In addition, confirmed that failed login attempts were recorded in the audit log in accordance with DoD 8500.2.</p> <p>Confirmed through inquiry and observation that audit trails were maintained for at least 5 years.</p> <p><u>DFAS</u></p> <p>Confirmed through inquiry that audit trails were maintained for the application.</p>	<p>No relevant exceptions noted.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			<p>Inspected available audit trails and determined that the activities of users with root access were logged. In addition, confirmed that failed login attempts were recorded in the audit log in accordance with DoD 8500.2.</p> <p>Confirmed through inquiry and observation that audit trails were maintained for at least 5 years.</p>	
27	<p>The contents of audit trails are protected against unauthorized access, modification, or deletion.</p>	<p><u>DECC SMC Mechanicsburg</u></p> <p>Contents of audit trails are protected in accordance with STIGs and the DISA Computing Services Security Handbook.</p> <p>User authorization for access to various systems is identified in each individual's new user agreement (completed when account is created).</p> <p><u>DFAS TSOPE</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>DISA</u></p> <p>Requested policy related to the protection of audit trails.</p> <p>Confirmed that policy limits access to audit trails to individuals with a need-to-know based on job responsibilities described on the SAAR form.</p> <p>Confirmed through inquiry and observation that audit logs included activities that might modify, bypass, or negate safeguards controlled by the system. In addition, confirmed that audit trails were protected against unauthorized access, modification, or deletion.</p> <p>Observed that only a select or limited number of individuals (including the Information Assurance Manager, the Assistant Information Assurance Manager, Database Administrator, and SA) had access to the audit trails.</p> <p><u>DFAS</u></p> <p>Requested policy related to the protection of audit trails.</p> <p>Confirmed that policy limits access to audit trails to individuals with a need-to-know based on job responsibilities described on the SAAR form.</p>	<p>No relevant exceptions noted.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			<p>Confirmed through inquiry and observation that audit logs included activities that might modify, bypass, or negate safeguards controlled by the system. In addition, confirmed the audit trails were protected against unauthorized access, modification, or deletion.</p> <p>Observed that only a select or limited number of individuals (including the Information System Security Officer and Information Assurance Manager) had access to the audit trails.</p>	
28	Tools are available to review audit records and generate reports from audit records.	<p><u>DECC SMC Mechanicsburg</u></p> <p>Tools are available for review through System Management Facility and ACF2 reports.</p>	<p><u>DISA</u></p> <p>Inquired with security personnel and inspected the audit tools available for reviewing audit records.</p> <p>Determined whether a reporting function is available and, if so, identified the types of reports being generated and reviewed.</p>	No relevant exceptions noted.
29	Actual or attempted unauthorized, unusual, or sensitive network access is monitored, and suspicious or irregular access activity is investigated, and appropriate action taken.	<p><u>DECC SMC Mechanicsburg</u></p> <p>ACF2 is maintained at DECC SMC Mechanicsburg and at the payroll offices by various SAs with differing roles (for example, administration or user accounts). The logs are centrally reviewed at DECC SMC Mechanicsburg. Multiple unsuccessful login attempts result in the account being locked. If the account is unused for a specified period, the account is deactivated.</p>	<p><u>DISA</u></p> <p>Obtained copies of the policies and procedures relating to access controls.</p> <p>Inquired with the SA to confirm that system access (including unauthorized, unusual, or sensitive access) was monitored.</p> <p>Inquired with the SA to confirm that suspicious or irregular access activity was investigated, and appropriate actions were taken.</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			Obtained and inspected evidence (including audit log reviews and incident reports) to confirm that investigations and actions were taking place.	
30	The acquisition, development, or use of mobile code in DoD systems meets current guidelines, standards, and regulations.	<u>DECC SMC Mechanicsburg</u> Use of mobile code is only permitted after a risk assessment, categorization of the mobile code, and counter measures have been implemented, and only when a waiver has been obtained from the responsible Chief Information Officer's office.	<u>DISA</u> Inspected the DoD systems guidelines, standards, and regulations concerning mobile code. Inquired with the SA to confirm that the acquisition, development, or use of mobile code in DoD systems meets current guidelines, standards, and regulations. Inspected the National Information Assurance Partnership website and confirmed that the website provided a list of approved products.	No relevant exceptions noted.
31	All servers, workstations, and mobile computing devices implement virus protection that includes a capability for automatic updates.	<u>DECC SMC Mechanicsburg</u> Anti-virus software is installed on personal computers, laptops, and systems under DECC SMC Mechanicsburg control.	<u>DISA</u> Observed that all servers, workstations, and mobile computing devices implement virus protection that included a capability for automatic updates at all DCPS locations. Obtained print screens as evidence that virus protection settings were configured.	No relevant exceptions noted.
32	All Virtual Private Network traffic is visible to the network IDS.	<u>DECC SMC Mechanicsburg</u> Information security scanner Real Secure is installed at various points that give visibility into the network traffic ingressing and egressing the DISA enclave.	<u>DISA</u> Inquired with the SA to confirm that all Virtual Private Network traffic was visible to the network IDS. Inspected the system network diagram and inquired of the SA to confirm that Virtual Private Network traffic was included on the diagram.	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
33	At a minimum, medium-robust 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.	<u>DECC SMC Mechanicsburg</u> Appropriate IA 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.	<u>DISA</u> Inquired with key personnel to confirm that at a minimum, medium-robust COTS IA and IA-enabled products were used to protect sensitive information when the information transits public networks or the system handling the information was accessible by individuals who were not authorized to access the information on the system for each of the DCPS locations.	No relevant exceptions noted.
34	Unless there is an overriding technical or operational problem, workstation screen-lock functionality is applied to each workstation.	<u>DECC SMC Mechanicsburg</u> Workstations are locked systematically after a period of inactivity in accordance with DoD Instruction 8500.2. A password is required to unlock the workstation. <u>DFAS TSOPE</u> The Desktop Management Initiative (not associated with TSOPE) controls the configuration of all DFAS computers, including the operating system and the application of screen-lock functionality.	<u>DISA</u> Confirmed with the Network Administrator the type of operating system personnel used. Confirmed through observation that workstation screen-lock functionality was applied. <u>DFAS</u> Confirmed with the Network Administrator the type of operating system personnel used. Confirmed through observation that workstation screen-lock functionality was applied.	<u>DECC SMC Mechanicsburg</u> Screen-lock functionality was not applied on 2 of 45 workstations inspected at DECC SMC Mechanicsburg. As a mitigating circumstance, DECC SMC Mechanicsburg has physical access controls in place that limit unauthorized access to workstations.
35	Instant messaging traffic to and from users that are independently configured by end users and that interact with a public service provider is prohibited within DoD information systems.	<u>DECC SMC Mechanicsburg</u> Use of instant messaging applications is not permitted and network personnel monitor common firewall and system ports to identify and eliminate the use of instant messaging applications.	<u>DISA</u> Inquired with personnel to confirm that policy prohibits the use of instant messaging. Inquired of network personnel the methods used to control instant messaging.	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		<p><u>DFAS TSOPE</u></p> <p>Desktop Management Initiative controls the configuration of computers so instant messaging programs are not authorized. TSOPE monitors application usage through an automated software auditing application that runs regularly when users login to their workstation. Instant messaging programs are identified as part of that auditing process.</p>	<p>Requested and inspected firewall rules to confirm instant messaging was blocked.</p> <p><u>DFAS</u></p> <p>Inquired with personnel to confirm that policy prohibits the use of instant messaging.</p> <p>Inquired of network personnel the methods used to control instant messaging.</p> <p>Requested and inspected firewall rules to confirm instant messaging was blocked.</p>	
36	<p>For automated information system applications, a list of all (potential) hosting enclaves is developed and maintained along with evidence of deployment planning and coordination and with the exchange of connection rules and requirements.</p>	<p><u>DECC SMC Mechanicsburg and DFAS TSOPE</u></p> <p>All interconnections of DoD information systems are managed continuously to minimize risk by ensuring that the assurance of one system is not undermined by vulnerabilities of interconnected systems.</p>	<p><u>DISA</u></p> <p>Inspected the DECC SMC Mechanicsburg SSAA to confirm the DCPS enclave was identified and documented.</p> <p><u>DFAS</u></p> <p>Inspected the Service-Level agreement between DISA and DFAS to confirm that deployment planning and coordination have been considered along with the exchange of connection rules and requirements.</p>	No relevant exceptions noted.
37	<p>Group authenticators for application or network access may be used only in conjunction with an individual authenticator.</p>	<p><u>DECC SMC Mechanicsburg and DFAS TSOPE</u></p> <p>Group authenticators are not used for DCPS or network access. Upon initial system login, a user's actions are tracked based on the individual's unique user account.</p>	<p><u>DISA</u></p> <p>Confirmed through inquiry that authenticators for application, networks, or operating systems were not used.</p> <p><u>DFAS</u></p> <p>Confirmed through inquiry that group authenticators for applications and networks were not used.</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
38	To help prevent inadvertent disclosure of controlled information, all contractors and foreign nationals are identified by e-mail addresses and display names.	<u>DECC SMC Mechanicsburg</u> Exchange Server Administration includes the specific configuration of e-mail addresses and display names for contractors and foreign nationals.	<u>DISA</u> Obtained a listing of contractors' and foreign nationals' e-mail addresses and display names to confirm that proper identification was present for those with access to DCPS.	No relevant exceptions noted.
39	Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using National Institute of Standards and Technology-certified cryptography.	<u>DECC SMC Mechanicsburg</u> Encryption data streams are in the process of conforming to standards in the Federal Information Processing Standards Publication 140-2, "Security Requirements for Cryptographic Modules."	<u>DISA</u> Inquired of security personnel whether DCPS data were transmitted through a commercial or wireless network.  Inquired of security personnel to confirm that National Institute of Standards and Technology cryptography was used to protect information when the information was transmitted over commercial or wireless networks.	<u>DFAS TSOPE</u> Sensitive but unclassified payroll and personnel data transmitted within DoD internal networks were not encrypted.  In addition, data transmitted outside DoD internal networks are not encrypted unless DFAS requests data encryption.
40	Discretionary access controls are a sufficient IA mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rules.	<u>DECC SMC Mechanicsburg</u> The DECC SMC Mechanicsburg enclave SSAA requires that access to all DoD information systems are based on a demonstrated need-to-know and is granted in accordance with applicable laws and DoD 5200.2-R for background investigations, special access, and IT position designations.  An appropriate security clearance and non-disclosure agreement are also required for access to classified information in accordance with DoD 5200.1-R.	<u>DISA</u> Inspected the ACF2 access list of all individuals who had direct access to the DCPS system software and selected a random sample 45 of users with direct access.	<u>DECC SMC Mechanicsburg</u> Of the 45 SAAR forms reviewed, 4 forms did not include justification for granting access to DCPS. In addition, 1 of the 45 SAAR forms reviewed did not indicate the organization requesting access for the user.



No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
41	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>DECC SMC Mechanicsburg</u> DECC SMC Mechanicsburg performs monthly retina scans to check for any DCPS network vulnerabilities. DCPS and its hardware are reviewed for STIG compliance through periodic SRRs that are conducted by the FSO on the DCPS mainframe domain.	<u>DISA</u> Confirmed through inquiry that conformance testing is performed and includes periodic, unannounced, in-depth monitoring, and provides for specific penetration testing to confirm compliance with all vulnerability mitigation procedures was planned, scheduled, and conducted.  Obtained and inspected documentation produced from this conformance testing (including information security scans) as evidence that penetration testing was completed.	<u>DISA FSO</u> An SRR was not completed within the last 3 years for the LPAR where the DCPS application was housed.
42	All users are warned that they are entering a Government information system.	<u>DECC SMC Mechanicsburg and DFAS TSOPE</u> All DISA networks and platforms present a message to users upon login, which warns them that they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording, and auditing.	<u>DISA and DFAS</u> Observed that workstations display a DoD warning banner.	No relevant exceptions noted.
43	Information and DoD information systems that store, process, transmit, or display data in any form or format that is not approved for public release comply with requirements in policy.	<u>DISA DECC SMC Mechanicsburg</u> Information on DoD systems that store, process, transit, or display data in any format that is not approved for public release complies with DoD policy.  Access to all DoD information systems is based on a demonstrated need-to-know and is granted in accordance with applicable laws and DoD 5200.2-R for background investigations, special access, and IT position designations.	<u>DISA</u> Observed and conducted a walk-through of the DECC SMC Mechanicsburg data center, including onsite tape storage areas, to confirm that labels indicating classification level were affixed to all computers and storage devices.  Inquired with security personnel to confirm that information in-transit through the network was encrypted.	<u>DFAS TSOPE</u> Sensitive but unclassified pay and personnel data transmitted within DoD internal networks were not encrypted.  In addition, data transmitted outside DoD internal networks are not encrypted unless DFAS requests data encryption.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
	Guidance documents and information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, are encrypted, at a minimum, with National Institute of Standards and Technology certified cryptography.		Inquired with security personnel to confirm the use of a network monitoring tool.	
44	Connections between DoD enclaves and the Internet or other public or commercial-wide area networks require a DMZ and boundary defense mechanisms (including firewalls and network IDSs) at the enclave boundary.	<p><u>DECC SMC Mechanicsburg</u></p> <p>Perimeter firewalls, routers, and IDSs are deployed.</p> <p>DoD information systems regulate access and remove access to the Internet by employing positive technical controls (including proxy services and screened subnets [also called a DMZ]) that are isolated from all other DoD information systems through physical means.</p>	<p><u>DISA</u></p> <p>Inspected the system architecture to confirm that connections between DoD enclaves and the Internet were configured with a DMZ and boundary defense mechanisms (including firewalls and network IDSs) at the enclave boundary.</p> <p>Inspected the system network diagram and inquired of the SA to confirm that a DMZ and other defense mechanisms are employed.</p> <p>Observed the existence of firewalls and IDS devices.</p>	No relevant exceptions noted.
45	Devices that display or output classified or sensitive information in human-readable form (monitors and printers) are positioned to deter unauthorized individuals from reading the information.	<p><u>DECC SMC Mechanicsburg</u></p> <p>Devices that display or output sensitive information are labeled to indicate whether sensitive information can be displayed.</p> <p><u>DFAS TSOPE</u></p> <p>Access to systems containing sensitive information display warning banners upon login to warn authorized users, and unauthorized users are denied access while attempting to login to the system.</p>	<p><u>DISA and DFAS</u></p> <p>Observed that monitors and printers displaying sensitive information were positioned to deter unauthorized individuals from reading the information.</p>	<p><u>DFAS TSOPE</u></p> <p>Printers at the DFAS TSOPE facility that output sensitive information in human-readable form were not properly positioned to deter unauthorized individuals from accessing or reading the information. As a mitigating circumstance, physical controls are in place at the facility restricting access to the unauthorized personnel.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		Individuals who print sensitive information in human-readable form have localized printers. Each user that prints sensitive data in human-readable form is accountable for security in handling that information.		
46	Individuals requiring access to sensitive information are processed for access authorization in accordance with DoD personnel security policies.	<p><u>DECC SMC Mechanicsburg</u></p> <p>The DECC SMC Mechanicsburg enclave 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. At a minimum, all DECC SMC Mechanicsburg employees (military, civilian, or contractors) will have a SECRET security clearance and a favorably completed National Agency check.</p>	<p><u>DISA</u></p> <p>Requested, obtained, and inspected the policies and procedures for gaining access to sensitive information.</p> <p>Obtained the ACF2 listing of all personnel with access to DCPS.</p> <p>Selected a random sample of 45 users with access to DCPS to inspect their SAAR forms to confirm that each SAAR form includes the user's justification for access, security clearance level, and approval from management.</p>	<p><u>DECC SMC Mechanicsburg</u></p> <p>Of the 45 SAAR forms reviewed, 4 forms did not include justification for granting access to DCPS. In addition, one of the 45 SAAR forms reviewed did not indicate the organization requesting access for the user.</p>
47	DoD information systems comply with DoD ports, protocols, and services guidance.	<p><u>DECC SMC Mechanicsburg</u></p> <p>DCPS-related ports, protocols, and services are configured according to DoD guidance.</p>	<p><u>DISA</u></p> <p>Inquired of DECC SMC Mechanicsburg personnel and observed network monitoring to confirm that DoD information systems comply with DoD ports, protocols, and services guidance, including all ports, protocols, and services whether currently active or planned for use.</p> <p>Confirmed that ports, protocols, and services were identified and registered.</p> <p>Inspected documentation to support that DCPS had gone through the DISA STIG process.</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
48	<p>Binary or machine-executable public domain software products and other software products with limited or no warranty are not used in DoD information systems.</p>	<p><u>DISA DECC SMC Mechanicsburg</u></p> <p>Public domain software products and other software products with limited or no warranty (including freeware or shareware) are only used in DoD information systems to meet compelling operational requirements.</p> <p>Those products are thoroughly assessed for risk and accepted for use by the responsible Designated Approving Authority.</p>	<p><u>DISA</u></p> <p>Inspected a listing of software products and confirmed through inquiry of management that the mainframe housing DCPS did not have binary or machine-executable public domain software and other software products with limited or no warranty installed on the mainframe.</p>	<p>No relevant exceptions noted.</p>
	<p><b><i>Application Software Development and Change Control</i></b></p>			
49	<p>A system development life cycle methodology has been implemented and documented.</p>	<p><u>DFAS TSOPE</u></p> <p>A defined configuration management process is in place at DFAS TSOPE. The process is documented in the DCPS SSAA, Appendix S. Included within the plan are:</p> <ul style="list-style-type: none"> <li>• formally documented configuration management roles, responsibilities, and procedures, including management of IA information and documentation;</li> <li>• detailed roles of the CCB, including its roles for reviewing and approving changes; and</li> </ul>	<p><u>DFAS</u></p> <p>Inspected the configuration management plan to confirm that the plan had been documented.</p> <p>Inquired of DFAS TSOPE personnel to confirm that a configuration management process was implemented and includes the following:</p> <ul style="list-style-type: none"> <li>• formally documented configuration management roles, responsibilities, and procedures, including management of IA information and documentation;</li> <li>• detailed roles of the CCB, including its roles for reviewing and approving changes; and</li> </ul>	<p>No relevant exceptions noted.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		<ul style="list-style-type: none"> <li>descriptions of the testing process that all changes must go through, including the migration of the change from the development region to the testing region and the testing region to production environment.</li> </ul>	<ul style="list-style-type: none"> <li>descriptions of the testing process that all changes must go through, including the migration of the change from the development region to the testing region and the testing region to production environment.</li> </ul>	
50	<p>Authorizations for software modifications are documented and maintained. This should also include emergency changes.</p>	<p><u>DFAS TSOPE</u>  A Configuration Management Plan is implemented for software modifications contained in the DFAS TSOPE Business Process Handbook, updated October 23, 2005.</p> <p>All modifications go through the system change request (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 change is run through the SCR process at the start of the next business day.</p>	<p><u>DFAS</u>  Requested the list of program code and database modifications made to the DCPS production code library during the period July 1, 2005, through June 30, 2006.</p> <p>We examined a random sample of 45 modifications to an approved SCR and confirmed through inspection that SCR was authorized by the Program Manager or Software Director. We also tracked each SCR identified above to the Release Authorization Report to confirm that it was approved by the Software Director.</p>	No relevant exceptions noted.
51	<p>Use of public domain and personal software is restricted.</p>	<p><u>DFAS TSOPE</u>  Does not allow any use of public domain or personal software. DCPS is housed on a DISA mainframe and all utilities necessary are on that mainframe.</p>	<p><u>DFAS</u>  Inspected policy (DCPS SSAA) to confirm that personal software is restricted.</p> <p>Requested a listing of approved software.</p> <p>Inquired with system personnel to determine how this requirement was enforced.</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
52	<p>Changes are controlled as programs progress through testing to final approval to ensure completeness, authorization, and software quality requirements and validation methods are focused on the minimization of flawed or malformed software.</p> <p>Software that can negatively impact integrity or availability (for example, buffer overruns) is specified for all software development initiatives.</p>	<p><u>DFAS TSOPE</u></p> <p>Testing changes follows the approved process outlined in the DFAS TSOPE Business Process Handbook prior to implementation.</p> <p>A Testing Deficiency Report is issued for SCRs with negative test results and the Testing Deficiency Report is routed to the appropriate individuals. If necessary, an amendment is issued and progresses through the same approval process as an SCR.</p>	<p><u>DFAS</u></p> <p>Using the same sample selected for control objective No. 50, we confirmed that the change followed the appropriate test and migration process by inspecting the following documents 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 of DCPS security personnel as to their roles and responsibilities for releasing security-related changes included in DCPS releases.</p> <p>Observed release notes for all major DCPS production releases that occurred July 1, 2005, through June 30, 2006.</p>	<p><u>DFAS TSOPE</u></p> <p>Of the 45 SCRs inspected, 7 changes did not include documented test results. Of the seven changes:</p> <ul style="list-style-type: none"> <li>• five were program code changes,</li> <li>• one was an SCR addendum, and</li> <li>• one was an interest rate table change.</li> </ul>
53	<p>Distribution and implementation of new or revised software is controlled.</p>	<p><u>DFAS TSOPE</u></p> <p>Release management staff is responsible for the distribution and implementation of new and revised software.</p>	<p><u>DFAS</u></p> <p>Using the same sample selected for control objective No. 50, we confirmed that the change followed the appropriate distribution process by inspecting the Release Authorization Report for completeness and authorization.</p>	<p>No relevant exceptions noted.</p>
54	<p>Programs are labeled and inventoried.</p>	<p><u>DFAS TSOPE</u></p> <p>Release management staff is responsible for ensuring that all programs are labeled and inventoried within the appropriate library.</p>	<p><u>DFAS</u></p> <p>Using the same sample selected for control objective No. 50, we confirmed that the changes had been labeled, assigned an identification number, and inventoried.</p>	<p>No relevant exceptions noted.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
55	Access to program libraries is restricted to appropriate personnel to ensure that the movement of programs and data among libraries is controlled.	<p><u>DFAS TSOPE</u></p> <p>The SA manages access rights to the program libraries and databases through ACF2. The Database Administrator grants access to the appropriate development or production environments through IDMS. IDMS controls the version of the software in the development and production environments.</p>	<p><u>DFAS</u></p> <p>Observed the DCPS Librarian to understand how the development and production libraries are controlled.</p> <p>Inspected the access control lists for the production and development libraries (directories) to confirm that only authorized personnel have access.</p>	<p><u>DFAS TSOPE</u></p> <p>DFAS TSOPE Database Administrators had unrestricted access and made changes directly to payroll data recorded in IDMS by using a Data Manipulation Language Online tool. Although those changes were recorded in an audit log, TSOPE management did not review those logs regularly to determine whether the changes were appropriate and approved.</p> <p>In addition, three active user accounts on the IDMS user access list were identified; however, those accounts were not associated with personnel who needed that type of access. Specifically, one account was for an individual no longer employed by DFAS TSOPE, one account was a duplicate account, and one account was for an individual that no longer required that level of access. However, as a mitigating circumstance, access to IDMS was controlled through the ACF2 utility. None of the three account holders had access to ACF2.</p>
56	Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end-user IA roles and responsibilities.	<p><u>DFAS TSOPE</u></p> <p>The Service-Level agreement between DFAS and DECC SMC Mechanicsburg explicitly states the IA roles and responsibilities of the customer and service provider.</p>	<p><u>DFAS</u></p> <p>Inspected the Service-Level agreement to confirm that the agreement expressly addresses Government, service provider, and end-user IA roles and responsibilities.</p>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		Data are collected to support reporting and IA management activities throughout the investment lifecycle.		
57	The acquisition of all IA and IA-enabled Government off-the-shelf IT products is limited to products that have been evaluated by NSA or are in accordance with NSA-approved processes.	<u>DFAS TSOPE</u> The System Support Office is responsible for reviewing and approving all COTS and Government off-the-shelf IT products.	<u>DFAS</u> Confirmed through inquiry that DFAS verified that products were verified by NSA or conducted an evaluation in accordance with NSA-approved processes for all IA-related products.  Inspected the National Information Assurance Partnership website and confirmed a list of approved products.	No relevant exceptions noted.
	<i>System Software Controls</i>			
58	Access authorizations are appropriately limited.	<u>DECC SMC Mechanicsburg</u> User accounts are suspended after 30 days of no activity (60 days for TSOPE and payroll offices) and are removed after 90 days. Accounts are issued by local SAs. User access administration controls are tested in multiple control objectives, primarily in the Access Control section of this report.	<u>DISA</u> Inspected the policies and procedures for restricting access to system software to confirm that they were up-to-date.  Obtained the ACF2 access list of all individuals who had direct access to system software and selected a random sample of 45 users with direct access.  For each user selected, confirmed with key management that those users were authorized to have this access.	No relevant exceptions noted.
59	Policies and techniques have been implemented for using and monitoring use of system utilities.	<u>DECC SMC Mechanicsburg</u> Access to system software is administered based on roles.	<u>DISA</u> Inquired with key DECC SMC Mechanicsburg personnel to confirm how root and privileged access was administered.  Obtained the list of individuals with root and privileged access.  Inquired with management that root and privileged access was reviewed	No relevant exceptions noted.



No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			<p>and approved and that the use of those accounts was logged.</p> <p>Inspected each audit log from the DCPS LPAR for the 12-month audit period to confirm that key personnel reviewed the logs on a regular basis and that any issues identified were documented and researched.</p> <p>Inspected the policies and procedures for monitoring system software and confirmed that they existed and were current.</p>	
60	<p>System software changes are authorized, tested, approved, and documented before implementation.</p>	<p><u>DECC SMC Mechanicsburg</u></p> <p>Procedures addressing the testing of patches, upgrades, and new automated information system applications are documented. All changes made at DECC SMC Mechanicsburg are captured in the Change Management System (Change Management 2000). Each change record includes the requested time and date of implementation, the action that is to occur, and justification for the action.</p> <p>All changes to information systems at DECC SMC Mechanicsburg are brought before at least one of two CCBs. DISA Headquarters has a executive software CCB, which 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 DECC SMC Mechanicsburg 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 and obtaining</p>	<p><u>DISA</u></p> <p>Obtained and inspected the change management policies and procedures for system software to confirm that they existed and were current.</p> <p>Obtained a list of all DCPS system software modifications that occurred July 1, 2005, through June 30, 2006, and selected a random sample of 45 modifications.</p> <p>For each modification selected, we obtained the change request documentation and confirmed that it was approved by key personnel before implementation.</p> <p>Confirmed that each modification was tested and the test results were approved before the modification was implemented.</p> <p>Confirmed that the modifications were documented by inspecting the SCR; System Test Plan; Detailed System Specifications; and Unit, System, and Acceptance testing results.</p>	<p><u>DECC SMC Mechanicsburg</u></p> <p>Test results were not documented prior to September 15, 2005. During that time, DECC SMC Mechanicsburg was in the process of developing policy requiring that this documentation be maintained in response to recommendations made during the FY 2005 DCPS Statement on Auditing Standard 70 audit. Therefore, the 13 sample changes selected during that time could not be provided. All changes that took place after September 15, 2005, were provided.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		<p>customer approval before proceeding. In addition, the local CCB is responsible for maintaining the change control records.</p> <p>The DISA executive software CCB consists of representative from DISA Headquarters, as well as all the DECCs. The DECC SMC Mechanicsburg local CCB consists of all department heads and the Information Assurance Manager.</p>		
61	<p>Good engineering practices with regards to the integrity mechanisms of COTS, Government off-the-shelf, and custom developed solutions are implemented for incoming and outgoing files.</p>	<p><u>DECC SMC Mechanicsburg</u></p> <p>Implemented COTS software that scans incoming and outgoing files to insure the integrity of those files.</p>	<p><u>DISA</u></p> <p>Confirmed through inquiry that a controlled interface was used for interconnections among DoD information systems that were connected to DCPS.</p> <p>Observed the existence of access control lists, IDS, firewalls, encryption, and network monitoring.</p> <p>Confirmed through inquiry that interface inputs were automatically validated by the system for missing information, format, consistency, and reasonableness.</p> <p>Inquired of personnel about the system batch file process for interface inputs of control totals and line counts.</p>	<p>No relevant exceptions noted.</p>

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
	<i>Segregation of Duties</i>			
62	Incompatible duties are identified and policies implemented to segregate those duties.	<u>DECC SMC Mechanicsburg and DFAS TSOPE</u> Developed distinct system support functions to ensure there is adequate segregation of duties.	<u>DISA and DFAS</u> Inspected the organizational chart and the job descriptions for IA positions at DECC SMC Mechanicsburg and DFAS TSOPE in relation to DCPS to confirm that there was appropriate segregation of duties and incompatible duties did not exist.  Inquired with management and inspected the organizational chart to confirm that the following distinct system support functions were performed by different individuals. Those functions include: <ul style="list-style-type: none"> <li>• information security management,</li> <li>• system design,</li> <li>• application programming,</li> <li>• systems programming,</li> <li>• quality assurance and testing,</li> <li>• library management and change management,</li> <li>• computer operations,</li> <li>• production control and scheduling,</li> <li>• data control,</li> <li>• data security,</li> <li>• data administration, and</li> <li>• network administration.</li> </ul>	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
63	System management job descriptions have been documented.	<u>DECC SMC Mechanicsburg and DFAS TSOPE</u> Developed position descriptions for distinct system support positions exist.	<u>DISA and DFAS</u> Inspected the job descriptions for the applicable types of personnel listed in control objective No. 62.	No relevant exceptions noted.
64	System management employees understand their roles and responsibilities.	<u>DECC SMC Mechanicsburg and DFAS TSOPE</u> Personnel receive and sign their position descriptions to confirm that they are aware of their proposed responsibilities.	<u>DISA and DFAS</u> Selected a random sample of 45 employees and confirmed through inquiry that they understood their roles and responsibilities.  Observed documentation to confirm that employees had signed position descriptions.	No relevant exceptions noted.
65	Management reviews effectiveness of control techniques.	<u>DFAS TSOPE</u> Management periodically reviews and updates security policies and procedures.	<u>DFAS</u> Inspected the DCPS Systems Security Policy, Security Requirements, and the Certification Test and Evaluation Plan and Procedures to confirm that each document was periodically updated.	No relevant exceptions noted.
66	Formal procedures guide system management personnel in performing their responsibilities.	<u>DECC SMC Mechanicsburg and DFAS TSOPE</u> Formal standard operating procedures for personnel who support DCPS have been developed and implemented.	<u>DISA and DFAS</u> Inspected standard operating procedures used by personnel in performing their job responsibilities with respect to DCPS.	No relevant exceptions noted.
67	Access procedures enforce the principles of separation of duties and "least privilege."	<u>DECC SMC Mechanicsburg and DFAS TSOPE</u> Privilege accounts are only used by DISA and DCPS personnel to create, modify, or delete user accounts.	<u>DISA and DFAS</u> Inspected the access control policies and procedures for compliance with the principles of separation of duties and "least privilege."	No relevant exceptions noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
68	Active supervision and review are provided for all system management personnel.	<u>DECC SMC Mechanicsburg</u> Support functions are organized based on job responsibility to ensure segregation of duties.	<u>DISA</u> Inspected the organizational chart to confirm that a management structure was established.  Inspected position descriptions of key DCPS support personnel to confirm supervisory responsibilities were established.	No relevant exceptions noted.

---

**Section IV: Supplemental Information Provided  
by DFAS and DISA**

---



## **Introduction**

DFAS and DISA have prepared this section and it is included to provide user organizations with information that 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 Statement on Auditing Standard 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 either the TSOPE or DECC SMC Mechanicsburg.

This information has not been subjected to the procedures applied to the examination 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 a plan to be implemented when a disaster or impending threat would render DCPS production support inoperable (for example, hurricanes or damage to TSOPE facilities due to fire). This plan is evaluated and updated on an annual basis. If an impending threat or event occurs, production support control for DCPS is transferred to an alternate-processing site. Currently, that site is the DISA Processing Element in Huntsville, Alabama. The COOP includes the names of DCPS staff members who will serve as a pool of resources to execute the plan, and it includes a list of documentation and supplies that are necessary to support the mobilized team.

The team is composed 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 divided into two smaller teams, with each team covering a 12-hour shift. Team leaders are appointed for the respective shift teams. TSOPE and DCPS project management staff coordinate and are involved in each step in planning and executing the COOP. Although this plan works for any type of disaster when production support becomes inoperable, it has been executed several times in the past few years during disastrous weather conditions, such as hurricanes.

### **DECC SMC Mechanicsburg Business Continuity Plans**

To accommodate a major disaster at any major DISA processing center, DISA has established an Enterprise Business Continuity Program. The DISA program uses multiple internal locations and, for mainframe processing, uses the Assured Computing Environment infrastructure elements located at DECC SMC Mechanicsburg and Ogden. DECC SMC Mechanicsburg 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. Recovery efforts for server-based elements are hosted at DECC Infrastructure Services Center St Louis.



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 IDMS, and related mid-tier servers and communication devices. Replicated data and backup tapes containing incremental daily and complete weekly backups are rotated offsite to designated locations for storage on a predetermined schedule.

The Crisis Management Team at DECC SMC Mechanicsburg 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 at DECC SMC Ogden. TSOPE personnel participate in the yearly COOP exercise to ensure that the process works correctly and that documentation is updated appropriately.

# Acronyms and Abbreviations

ACF2	Access Control Facility 2
CCB	Configuration Control Board
COOP	Continuity of Operations Plan
COTS	Commercial off-the-shelf
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
DMZ	Demilitarized Zones
DoD	Department of Defense
EOP	Executive Office of the President
EPA	Environmental Protection Agency
FSO	Field Security Operations
IA	Information Assurance
IDMS	Integrated Database Management System
IDS	Intrusion Detection System
IT	Information Technology
LPAR	Logical Partition
MAC	Mission Assurance Category
NSA	National Security Agency
OIG	Office of the Inspector General
OLQ	Online Queries
SA	System Administrator
SAAR	Systems Access Authorization Request
SCR	System Change Request
SMC	System Management Center
SMO	System Management Office
SRR	Security Readiness Review
SSAA	System Security Authorization Agreement
STIG	Security Technical Implementation Guide
TSOPE	Technology Services Engineering Organization in Pensacola
TSP	Thrift Savings Plan
VMS	Vulnerability Management System

# **Report Distribution**

## **Office of the Secretary of Defense**

Under Secretary of Defense for Acquisition, Technology, and Logistics  
Under Secretary of Defense (Comptroller)/Chief Financial Officer  
Deputy Chief Financial Officer  
Deputy Comptroller (Program/Budget)  
Assistant Secretary of Defense for Networks and Information Integration/DoD Chief  
Information Officer  
Director, Program Analysis and Evaluation

## **Department of the Navy**

Naval Inspector General  
Auditor General, Department of the Navy

## **Department of the Air Force**

Auditor General, Department of the Air Force

## **Combatant Command**

Inspector General, U.S. Joint Forces Command

## **Other Defense Organizations**

Director, National Security Agency  
Director, Defense Finance and Accounting Service  
Inspector General, Defense Information Systems Agency

## **Non-Defense Federal Organizations and Individuals**

Office of Management and Budget  
General Accountability Office

## **Congressional Committees and Subcommittees, Chairman and Ranking Minority Members**

Senate Committee on Appropriations  
Senate Subcommittee on Defense, Committee on Appropriations  
Senate Committee on Armed Services  
Senate Committee on Homeland Security and Governmental Affairs  
House Committee on Appropriations  
House Subcommittee on Defense, Committee on Appropriations

## **Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (cont'd)**

House Committee on Armed Services

House Committee on Government Reform

House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform

House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform

House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

## **Team Members**

The Defense Financial Auditing Service, Department of Defense Office of Inspector General, in conjunction with contract auditors from Acuity Consulting, Inc., produced this report. Personnel from the Technical Assessment Division and Quantitative Methods Division, DoD OIG, also contributed to the report.

Paul J. Granetto  
Patricia A. Marsh  
Michael Perkins  
Kenneth H. Stavenjord  
Frank C. Sonsini  
Sean J. Keaney  
Anh H. Tran  
Charles S. Dekle  
Ernest G. Fine  
Travis R. Schenck  
Mary A. Hoover  
Nicholas Drotar, Jr  
Debra J. DeJonge  
Steve L. Kohne  
Alberto J. Calimano-Colon