Report No. D-2007-133 September 28, 2007

Inspector General

United States Department of Defense

Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness for the Period of July 1, 2006 Through June 30, 2007

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 Ms. Holly Williams at (703) 325-3557 (DSN 221-3557) or Ms. Donna A. Roberts at (703) 428-1070 (DSN 328-1070).

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 www.dodig.mil/hotline

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

September 28, 2007

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: Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness for the Period July 1, 2006, through June 30, 2007 (Report No. D-2007-133)

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

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Holly Williams at (703) 325-3557 (DSN 221-3557) or Ms. Donna A. Roberts at (703) 428-1070 (DSN 328-1070). 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

Foreword i

Section I

Independent Service Auditor's Report 1

Section II

Description of DCPS Operations and Controls Provided by DFAS and DISA 13

Section III

Control Objectives, Control Activities, and Tests of Operating Effectiveness 23

Section IV

Supplemental Information Provided by DFAS and DISA 117

Acronyms and Abbreviations 121

Report Distribution 123

Foreword

This report is intended for the use of Defense Finance and Accounting Service (DFAS) and Defense Information Systems Agency management, its user organizations, and the independent auditors of its user organizations. Department of Defense 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.

The Department of Defense, Office of Inspector General (DoD OIG) is implementing a long range strategy to conduct audits of DoD financial statements. The Chief Financial Officer's Act of 1990 (P.L. 101-576), as amended, mandates that agencies prepare and conduct audits of financial statements, which is key to achieving the goals of the Chief Financial Officers Act.

The DCPS is a pay processing system used to pay DoD civilian employees, as well as employees at several other Federal entities, including the Departments of Energy, Health and Human Services, and the Executive Office of the President. As of June 30, 2006, DCPS processed pay for approximately 798,000 employees.

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

Section I: Independent Service Auditor’s Report

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

SEP 28 2007

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: Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness for the Period July 1, 2006, through June 30, 2007

We have examined the accompanying description of the general computer and application controls related to the Defense Civilian Pay System (DCPS) (Section II). The Defense Finance and Accounting Service-Headquarters (DFAS-HQ) provides management control and coordination within DoD and has overall responsibility for implementation and application of DCPS. DCPS is maintained and supported by the DFAS technical support elements and the 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 about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the controls at DFAS and DISA that may be relevant to a DCPS user organization's internal controls as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and user organizations applied those aspects of internal controls contemplated in the design of the controls at DFAS and DISA; and (3) such controls had been placed in operation as of June 30, 2007.

The control objectives were specified by the Department of Defense Office of the Inspector General (DoD 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 DCPS general computer control environment includes certain controls that are pervasive across the DISA Defense Enterprise Computing Center (DECC) Mechanicsburg data center that houses DCPS. These types of pervasive controls include:

- overall security planning (e.g., DECC risk assessments, site security plans, security management structure);
- general employee processes (e.g., background investigations, position and job descriptions);
- group authentication;
- physical security;

- network administration (for example, firewalls, network scans, remote access, network monitoring, use of mobile code);
- incident response;
- environmental controls; and
- hardware maintenance.

The accompanying description does not include control objectives and control activity descriptions related to these pervasive controls, and our examination did not extend to these controls at the DISA DECC Mechanicsburg data center.

The accompanying description includes only those application control objectives and related controls resident at the Charleston, South Carolina; Pensacola, Florida; Indianapolis, Indiana; and Denver, Colorado Payroll Offices. DCPS processes approximately 81 interface files from DoD and external systems. Examples of these interface systems include the Defense Civilian Personnel Data System, Federal Reserve, Thrift Savings Plan, and the Department of Treasury. The accompanying description does not include control objectives and general and application controls related to the systems that interface with DCPS. Our examination did not extend to the controls resident at the National Security Agency (NSA) and Cleveland, Ohio Payroll Offices and controls-related systems that interface with DCPS. Furthermore, because of the sensitive nature of the pay 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 Department of Veterans Affairs (VA) payees on September 16, 2006, at the Pensacola, Florida Payroll Office. The payroll processing responsibilities were moved to the Indianapolis, Indiana Payroll Office as of May 13, 2007. Therefore, our examination only covered controls in place for VA payroll processing at the Pensacola, Florida Payroll Office for the period of August 20, 2006, to May 12, 2007, and only covered controls in place for the VA payroll processing at Indianapolis, Indiana Payroll Office for the period of May 13, 2007, to June 30, 2007.

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). Business continuity plans and procedures at DFAS and DISA, as provided by DFAS and DISA respectively 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 the 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, 2007. 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, 2006, through June 30, 2007. 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 such user organizations.

In performing our examination, we identified the following operating effectiveness deficiencies 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 every DCPS user to complete a System Access Authorization Request (SAAR) form. The SAAR form documents user access and must be signed by a supervisor indicating that such access has been approved. Upon examining a selection of 42 forms for DCPS non-payroll office users, we identified:

- 1 form had a user type that did not match the user type in the list of DCPS Users by Database;
- 3 forms had authorization types that did not match the authorization type in the list of DCPS Users by Database;
- 3 forms were missing the DCPS Security Awareness Computer-Based Training (CBT) completion date;
- 1 form was missing the user's signature;
- 1 form was missing the supervisor's signature;
- 9 forms were missing the date of the supervisor's signature;
- 5 forms were missing the security manager's signature; and
- 10 forms were missing the date of the security manager's signature.

Upon examining a selection of 42 forms for DCPS payroll office users, we identified:

- 6 forms had a user type that did not match the user type in the list of DCPS Users by Database;
- 3 forms had authorization types that did not match the authorization type in the list of DCPS Users by Database;
- 1 form was missing the DCPS Security Awareness CBT completion date;
- 2 forms were missing the supervisor's signature;
- 12 forms were missing the date of the supervisor's signature;

- 2 forms were missing the security manager's signature; and
- 4 forms were missing the date of the security manager's signature.

As a result, the following control objectives that rely on this control may not have been achieved during the period of July 1, 2006, through June 30, 2007:

"Controls prevent unauthorized system access to DCPS data."

"Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA General Computer Control (GCC) locations are valid, accurate, authorized, complete, [and] timely, support financial reporting requirements and provide sufficient audit trails."

Monitoring DCPS Error Reports

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

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

At the DFAS Pensacola Payroll Office, 16 of the 45 PIIRs selected from the CP1 and ZKA databases could not be located. Of the remaining 29 reports inspected, we identified:

- 8 reports were missing the technician's signature on the report;
- 8 reports were missing the date of when the report was annotated by the technician (WP 2600.19, "Summary" tab, Results, Exception box, cell G39); and
- 29 reports were inconsistently annotated with codes outlined in the SOP.

We confirmed that the requirement for technicians to annotate every transaction did not take effect until May 27, 2007. Only one report in the random sample was generated after this date (June 18, 2007). We scanned this report and noted that the technician who annotated this report did not comply with the new requirement and did not annotate transactions consistently. None of the 29 reports reviewed contained sufficient detail to confirm resolution of all the errors in the reports.

At the DFAS Denver Payroll Office, we inspected a sample of 45 PIIRs for the OMA and ZPA pay databases. For 5 of the 45 reports for the OMA database, the payroll office technician had not annotated each line item describing the correction method. Of the 45 reports inspected for the ZPA database, 1 report could not be located at the Denver Payroll office..

DCPS began processing pay for the Department of Veterans Affairs (VA) payees on September 16, 2006, at the Pensacola, Florida Payroll Office. The payroll processing responsibilities were moved to the Indianapolis, Indiana Payroll Office as of May 13, 2007. Therefore, our examination only covered controls in place for VA payroll processing at the Pensacola, Florida Payroll Office for the period of August 20, 2006, to

May 12, 2007, and only covered controls in place for the VA payroll processing at Indianapolis, Indiana Payroll Office for the period of May 13, 2007, to June 30, 2007.

At the DFAS Indianapolis Payroll Office, we inspected a sample of 25 PIIRs. The ZPV PIIR processing was performed at the Pensacola Payroll Office from August 20, 2006, through May 12, 2007. The Pensacola Payroll Office was unable to supply PIIR documentation for August 20, 2006, through January 19, 2007; therefore, testing could not be conducted for this timeframe. Of the 26 PIIRs in the DFAS Indianapolis Payroll Office sample, we observed:

- 1 report could not be provided;
- 15 reports were missing dates;
- 1 report was missing a technician's signature; and
- 4 reports were not properly annotated.

In addition, we observed that the PIIR did not contain sufficient detail documenting whether all errors were resolved.

As a result, the following control objective that relies on this control may not have been achieved during the period of July 1, 2006, through June 30, 2007:

"Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA (GCC) locations are valid, accurate, authorized, complete, [and] timely, support financial reporting requirements and provide sufficient audit trails."

Visitor Access

At the DFAS Denver Payroll Office, visitors with a valid Common Access Card (CAC), law enforcement badge, or military identification can enter the DFAS building and are not required to sign in and out with security; therefore, access is not limited to authorized payroll office personnel. We observed that data entry terminals were not located in physically secure locations within locked rooms. The data entry terminals are located in an open space shared by non-payroll personnel who may be able to access sensitive payroll information. In addition, we inspected a sample of 45 visitor logs. Of the 45 visitor logs inspected, we observed that:

- 14 logs did not have a telephone number recorded; and
- 2 logs did not have an escort's signature.

At the DFAS Indianapolis Payroll Office, visitors with a valid CAC, law enforcement badge, or military identification can enter the DFAS building and are not required to sign in and out with security; therefore, access is not limited to authorized payroll office personnel. We observed that terminals that process payroll are located within a physically secure building; however, terminal rooms are not locked and data entry terminals are connected to the system 24 hours a day, seven days a week. The terminal rooms are located in shared spaces with other agencies and non-payroll office personnel who may be able to access sensitive payroll information. In addition, we observed that visitors to the DFAS Indianapolis Payroll Office must sign in and out with authorized security personnel; however, once the visitor is inside the building there is no requirement to display the visitor badge.

As a result, the following control objective that relies on this control may not have been achieved during the period of July 1, 2006, through June 30, 2007:

"Controls prevent unauthorized physical access to DCPS data."

Limit and Reasonableness Checks

At the Indianapolis Payroll Office, we scanned the Less than $1 Greater than $5,000 Desk Guide and confirmed it did not have documented procedures requiring a supervisor to review 10% of the entries in the report, or the requirement to evidence the review with a signature or similar notation.

As a result, the following control objective that relies on this control may not have been achieved during the period of July 1, 2006, through June 30, 2007:

"Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA (GCC) locations are valid, accurate, authorized, complete, [and] timely, support financial reporting requirements and provide sufficient audit trails."

Gross Pay Change Reasonableness Check

At the DFAS Charleston Payroll Office, we observed that large payroll increases occurred in the pay periods ending March 17, 2007, and May 12, 2007, for the ZPD payroll database and the ZFR payroll database respectively. DFAS Charleston stated that these large increases were for annual pay bonuses that were paid in the appropriate pay period. However, DFAS Charleston was unable to provide us documentation to confirm the reasonableness of the large payroll increases. DFAS does not have a limit or reasonableness check to identify variances at the gross payroll level.

As a result, the following control objective that relies on this control may not have been achieved during the period of July 1, 2006, through June 30, 2007:

"Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA (GCC) locations are valid, accurate, authorized, complete, [and] timely, support financial reporting requirements and provide sufficient audit trails."

Personnel/Payroll Reconciliation Reports

At the DFAS Pensacola Payroll Office, we observed that the Payroll Office does not send a letter of completion signed by the supervisor to the personnel offices as documented in the Standard Operating Procedure (SOP). We inspected 45 Personnel/Payroll Reconciliation Reports. Of the 45 Personnel/Payroll Reconciliation Reports inspected, one report for Thrift Savings Plan (TSP) changes, which is handled by the Support Services Branch, could not be located. In addition, we observed that reports sent to the Support Services Branch were not maintained with a cover sheet as required by the SOP and that four reports were not completed within 10 working days as required by the SOP.

At the DFAS Charleston Payroll Office, we observed DFAS Charleston did not receive any Personnel/Payroll Reconciliation Reports for three of the four quarters of our audit period and received only four reports for another quarter. The most recent quarter reports were supplied; however, we were unable to test them as the reconciliation process was not yet complete. We observed, for the reports that were supplied, that the Charleston Payroll Office did not create cover sheets for the Personnel/Payroll Reports as required by the DFAS entity-wide Personnel/Payroll Reconciliation SOP.

As a result, the following control objective that relies on this control may not have been achieved during the period of July 1, 2006, through June 30, 2007:

"Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA (GCC) locations are valid, accurate, authorized, complete, [and] timely, support financial reporting requirements and provide sufficient audit trails."

"592" Reconciliation Reports

The "592" Reconciliation process is performed at the end of every pay period by Civilian Pay Technicians to confirm all balancing spreadsheets have been received and all discrepancies have been identified and/or corrected in order to release payroll files.

At the DFAS Pensacola Payroll Office, we inspected 26 592 reconciliation reports for both the CP1 and ZKA databases. For the CP1 database, we observed that one of the reports did not have a Certifying Officer's signature. For the ZKA database, we observed that 2 of the 2812 Statements of Withholding forms were not signed and dated, and 3 of the 2812 Statements of Withholding forms were not dated.

At the DFAS Charleston Payroll Office, we inspected 26 592 reconciliation reports for the ZGT payroll database. We observed that one of the reports was corrected by the preparer but not reconciled. Another report did not balance even when a supplemental was prepared, and it did not have the 592 preparer's signature. Three reports were corrected but did not balance and did not have a corresponding supplemental worksheet. When a correction to the 592 Report is necessary (that is, adjustments), a supplemental 592 is created to maintain the integrity of the original 592 Report. In addition, there is inconsistency in the DFAS Charleston Payroll Center's procedure for recording adjustments to the 592 when the report is initially out of balance or does not include all of the lines of accounting that are required for full reconciliation. We also observed that a policy and/or procedure does not exist that requires the 592 reconciler to identify an increase in total payroll or to document and include the reason for an increase in the 592 file when one occurs.

At the DFAS Indianapolis, Indiana Payroll Office, we inspected 26 592 reconciliation reports for the ZPV payroll database. Of the 26 592 reconciliation reports, 5 were processed by the VA; therefore, only 21 592 reports were tested. Of the 21 592 reconciliation reports selected, 2 Withholding Reports were not signed. In addition, policies and procedures for reconciling the 592 reports are not consistent.

As a result, the following control objectives that rely on this control may not have been achieved during the period of July 1, 2006, through June 30, 2007:

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

"Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA (GCC) locations are valid, accurate, authorized, complete, [and] timely, support financial reporting requirements and provide sufficient audit trails."

DCPS Interfaces

All DCPS interfaces should have a signed Memorandum of Agreement (MOA) documenting key information, including impacted parties, interconnection requirements, points of contact, security requirements, technical platform information, interface file information, and designated signatories. However, 4 of 81 DCPS interfaces did not have a documented MOA in place. In addition; DCPS data traveling within the NIPRNET (unclassified DISA network) was not encrypted.

As a result, the following control objectives that rely on this control may not have been achieved during the period of July 1, 2006, through June 30, 2007:

"DFAS has classified all DFAS-owned assets according to criticality and sensitivity."

"Data management and the disposition and sharing of data requirements are identified in the Service Level Agreements."

DCPS Password Configurations

All passwords for DCPS accounts are required to comply with Department of Defense Instruction 8500.2 "Information Assurance (IA) Implementation" standards. However, DCPS was not configured to enforce the use of complex passwords or to enforce the requirement to change at least four characters of the password.

As a result, the following control objective that relies on this control may not have been achieved during the period of July 1, 2006, through June 30, 2007:

"Passwords, tokens, or other devices are used to identify and authenticate users."

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, 2006, through June 30, 2007.

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 effective as of June 30, 2007, and information about tests of their operating effectiveness covers the period of July 1, 2006, through June 30, 2007. 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 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:

Patricia A. Marsh
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

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. DFAS began paying the Executive Office of the President (EOP) in 1998. The 2001 President's Management Agenda e-Payroll initiative established Federal payroll providers to service the entire executive branch of the Federal Government. DFAS was selected as one of those providers. DFAS began processing payroll for the Department of Energy (DOE) in 2003, the Department of Health and Human Services (HHS) in 2005, and the Environmental Protection Agency (EPA), Department of Veterans Affairs (VA) and the Broadcast Board of Governors (BBG) in 2006. As of June 30, 2006, DCPS currently processes pay for approximately 798,000 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.

Currently, DFAS is participating in a Base Realignment and Closure (BRAC) transformation that impacts the DCPS Payroll Offices. Approximately 250 payroll processing personnel at 3 DFAS Payroll Offices located in Pensacola, Florida; Charleston, South Carolina; and Denver, Colorado use DCPS. Approximately 150 processing personnel will use DCPS at the enduring payroll office sites located in Cleveland, Ohio, and Indianapolis, Indiana. DCPS is also used at NSA.* Additional users include Customer Service Representatives (CSRs) at customer activities and sites. Four of the five DFAS payroll offices process payroll for DoD civilians. The Pensacola Payroll Office processes EOP payroll. The Charleston Payroll Office processes DOE, HHS, and BBG payroll. The Indianapolis Payroll Office processes VA payroll, and the Denver Payroll Office processes EPA payroll. Migration completion of all payroll processing is targeted for June 2008.

* The NSA payroll office is not included in the scope of this "Description of DCPS Operations and Controls Provided by DFAS and DISA".

DCPS Support Functions

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

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

DCPS Systems Architecture

A two-tiered architecture comprises DCPS:

- mainframe hardware and software components - used as a repository for collecting and accumulating data, and providing centralized, biweekly processing of civilian pay and its attendant functions (for example, electronic funds transfer, generation of leave and earnings statements); and

- remote user/print spooler hardware and software - used to collect and/or pre-process data at customer sites, provide connectivity to DCPS mainframe components, and support printing of mainframe-generated outputs (for example, reports, timesheets) at customer locations. The components are largely customer-owned and operated, and include local area networks (LANs), personal computers, and a diverse assortment of printers and software that operates and connects the networks, computers, and printers. DFAS maintains a limited number of mid-tier (minicomputer) systems at selected DFAS sites to handle specialized printing requirements (for example, paychecks). Other offloaded print services, such as bulk printing for DCPS Payroll Offices and printing of Leave and Earnings Statements, are performed on PC/workstation hardware maintained by the Document Automation & Production Service (DAPS) located at various sites in the United States and overseas.

The two tiers of the DCPS architecture are connected via DoD-maintained networks composed of Internet Protocol (IP)-based systems for example, 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 PCs) that supply or exchange data with DCPS, mainly through electronic file transfers, on a regular basis. Examples of external interface sites include the Defense Civilian Personnel Data System, Thrift Savings Plan (TSP), Department of the Treasury, and non-DoD users such as DOE, EPA, EOP, HHS, BBG and VA.

The main technical components of DCPS include the following attributes:

- DCPS is housed in a separate logical domain on an IBM z9 mainframe computer located at DECC Mechanicsburg;
- the IBM mainframe operating system software is Z/OS release 1.7;
- DCPS is written in Common Business Oriented Language II;
- first point of entry security protection mechanisms are provided by Access Control Facility 2 (ACF2);
- DECC 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 (ID) and passwords; and
- third-party software packages are used for DCPS process scheduling and monitoring, tax calculations, and mailing address verification.

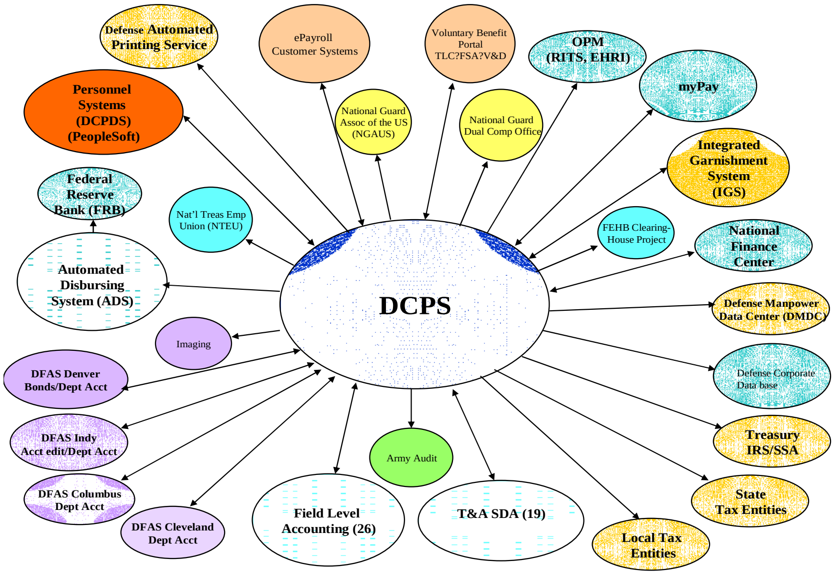
The payroll offices and associated Customer Service Representatives (CSRs) have access to DCPS via dedicated leased lines, various DoD networks, and through Secure Web Access. Secure Web Access enables secure transaction processing across the Non-Classified Internet Protocol Router Network. IBM's Host 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, (DoD I 8500.2) identifies specific control requirements DoD systems should achieve based on their designated Mission Assurance Category (MAC). The DCPS application Authority to Operate, dated July 29, 2005, is on file with the DFAS Chief Information Officer. According to the current DCPS SSAAs, as of June 30, 2005, the MAC level for the DCPS application is "MAC III" and its supporting enclave at DISA DECC Mechanicsburg is "MAC II."

DCPS Data Flow

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

DCPS Interfaces


Defense Automated Printing Service
ePayroll Customer Systems
Voluntary Benefit Portal TLC?FSA?V&D
OPM (RITS, EHRI)
myPay
Personnel Systems (DCPDS) (PeopleSoft)
National Guard Assoc of the US (NGAUS)
National Guard Dual Comp Office
Integrated Garnishment System (IGS)
Federal Reserve Bank (FRB)
Nat’l Treas Emp Union (NTEU)
FEHB Clearing-House Project
National Finance Center
Automated Disbursing System (ADS)
DCPS
Defense Manpower Data Center (DMDC)
Imaging
DFAS Denver Bonds/Dept Acct
Defense Corporate Data base
DFAS Indy Acct edit/Dept Acct
Treasury IRS/SSA
Army Audit
DFAS Columbus Dept Acct
State Tax Entities
DFAS Cleveland Dept Acct
Field Level Accounting (26)
T&A SDA (19)
Local Tax Entities

Overview of System Interfaces

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

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

- update personnel information;
- upload time and attendance data;
- download information for checks to be printed;
- report accounting information to the Department of the Treasury;
- reconcile enrollment information with health care providers; and
- download general accounting information to DoD agencies.

Automatic electronic 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, by way of communication lines of files written to magnetic tape at the host (using 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 the DCPS 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 Mechanicsburg, Pennsylvania. DECC 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. DFAS and DISA are Defense agencies that report to the Office of the Secretary of Defense.

Personnel Policies and Procedures

DFAS Payroll Offices and TSOPE.   Payroll office employees and contractors are required to review applicable administrative orders, policies, and procedures with the Human Resource Office and must complete appropriate forms to gain access to DFAS systems. New employees must meet with the Information Security (IS) Manager. The IS Manager is responsible for: (1) providing basic system security awareness training, (2) securing civilians' and contractors' signatures on an Automated Data Processing Security Awareness disclosure form, (3) identifying who an employees' Terminal Area Security Officer (TASO) is and what the TASO responsibilities are, and (4) notifying appropriate personnel when personnel actions occur. Those actions include providing access to or immediately terminating employee or contractor access to DFAS automated information system resources. The payroll offices and TSOPE facilities require a background check before a candidate can become an employee.

DECC Mechanicsburg. The security manager is responsible for processing new employees and contractors who are given access to DECC 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. For contractors, the security manager is responsible for confirming that all contractors are assigned to a valid contract, and have been approved to work at DECC 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 with which they must comply. New employees and contractors are required to complete a DD Form 2875, “System Authorization Access Request” to gain access to DISA systems. The security manager is responsible for processing those forms and confirming that the person requesting access has the proper clearance for the level of access requested. For contractors, the security manager confirms the length of the contract and determines when system accounts should expire. All new employees and contractors must complete security awareness training.

C. Monitoring

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

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

Field Security Operations. The Field Security Operations (FSO) unit conducts periodic System Readiness Reviews of DISA systems to determine whether those systems comply 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, established a standard Department-wide process, set of activities, general tasks, and management structure to certify and accredit information systems that will maintain the information assurance and security posture of the Defense Department information infrastructure throughout the life cycle of each system. The certification process is a comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards to establish the extent to which a particular design and implementation meet[s] 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 issued on June 30, 2005, and is valid for 3 years. The DECC SMC Mechanicsburg enclave SSAA was issued on February 27, 2006, and is valid for 3 years. The DCPS application Authority to Operate (ATO), dated 29 July 2005, is on file with the GS4B3 Information Assurance Manager. The DCPS ATO will be included in the annual SMC Mechanicsburg Unclassified Enclave SSAA package update that is submitted to the DISA Designated Approval Authority (DAA).

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 periodic 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 DOE, EPA, EOP, HHS, BBG and VA. Payroll processing involves approximately 81 data files that interface with DCPS. Those interfaces are linked to other DoD financial systems, as well as external systems. The majority of the interfaces is automated and must conform to documented interface specifications developed by the TSOPE.

The TSOPE is responsible for executing and monitoring all DCPS automated interfaces.

The support relationship between DFAS and DECC 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 SMC meet weekly to discuss DCPS processing issues. The Configuration Control Board, composed of customer agencies, SMC, 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 to communicate those issues and problems to SMC for resolution.

F. Control Activities

The DCPS control objectives and related control activities are included in Section III of this report, “Control Objectives, Control Activities, and Tests of Operating Effectiveness,” to eliminate the redundancy that would result from listing them in this section and 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 that:

- the servicing payroll office is notified of all terminated employees with access to DCPS;
- the local human resource office is notified of all terminated employees to ensure 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;
- if an alternative to the real Social Security Number (SSN) (“pseudo SSN”) is created, the created number has been authorized by appropriate user organization personnel and, if necessary, is accurately tied to a primary and valid SSN;
- user organization managers review the “Control of Hours” and other payroll-related reports for appropriateness and accuracy;
- all invalid time entry interface feeds are reviewed and processed by appropriate user organization personnel in a controlled manner; and
- all invalid personnel record interface feeds are resolved in the interface system by user organization personnel with appropriate approval by user organization management.

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

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

A. Scope Limitations

The control objectives documented in this section were specified by the DoD OIG. As described in 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. However, we did perform procedures to evaluate DCPS controls concerning interface input and output.

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 prevent unauthorized physical access to DCPS data.	1.1 - Policies and procedures are documented to describe that personnel payroll records and other sensitive information are 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.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** No relevant exception noted.
		1.2 - 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 stored properly in environmentally secure containers.	**DFAS Pensacola** We noted during an observation of the document storage warehouse, that one of the cipher-locked doors was propped open. We noted electronic records, such as CDs, are stored in the locked Pensacola Payroll Office;

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				however, are not required to be locked in a cabinet. DFAS Management indicated that the testing exceptions reflected office closure preparations as a result of BRAC and were not significant enough to qualify the control objective as these storage areas are located within the secure Payroll Office locations. **DFAS-Charleston** We noted during an observation of the document storage warehouse that access to the document storage warehouse was through swinging doors, which permit unauthorized physical access to personnel payroll records. The document storage warehouse is shared by business lines other than the payroll office. We noted electronic records such as tapes, microfilm, and CDs have not been used for 4 years

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				and are stored in an unlocked room in the Charleston Payroll Office, which is accessible to all Civilian Payroll employees. DFAS Management indicated the testing exceptions reflected office closure preparations as a result of BRAC and were not significant enough to qualify the control objective as these storage areas are located within the secure Payroll Office locations. **<u>DFAS-Denver</u>** No relevant exception noted. **<u>DFAS-Indianapolis</u>** No relevant exception noted.
		1.3 - All visitors to the Payroll Office must sign in and out with the authorized security personnel.	Inquired with appropriate personnel, obtained and inspected a sample of 45 visitor logs to the payroll office to confirm visitors must sign in with authorized security personnel.	**<u>DFAS-Pensacola</u>** No relevant exception noted. **<u>DFAS-Charleston</u>** No relevant exception noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<u>DFAS-Denver</u> Visitors with a valid Common Access Card (CAC), law enforcement badge, or military identification can enter the DFAS building and are not required to sign in and out with security; therefore, access to the payroll office is not limited to authorized personnel. Of the 45 visitor logs inspected: • 14 out of 45 Visitor/Employee Register Logs did not have a telephone number recorded. • 2 out of 45 Visitor/Employee Register Logs did not have an escort's signature. **<u>DFAS-Indianapolis</u>** We confirmed visitors to the DFAS Indianapolis Payroll Office must sign in and out with authorized security personnel; however, once the visitor

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				is inside the building there is no requirement to display the visitor's badge. Additionally, visitors with a valid Common Access Card (CAC), law enforcement badge, or military identification can enter the DFAS building and are not required to sign in and out with security; therefore, access to the payroll office is not limited to authorized personnel.
		1.4 - All terminals and payroll records are located in physically secured locations.	Inquired with appropriate personnel and observed the terminal rooms to confirm they are physically secure.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** We noted data entry terminals were not located in physically secure locations within locked rooms. The data entry terminals are located in an open space shared by non-payroll personnel who may

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				still be able to access sensitive payroll information. **DFAS-Indianapolis** Based on the procedures performed, the terminals are located within a physically secure building; however, terminal rooms are not located in physically secured locations within locked rooms, and data entry terminals are connected to the system 24 hours a day, 7 days a week. The terminals are located in shared spaces with other agencies and non-payroll office personnel, increasing the risk of unauthorized access to sensitive payroll information.
		1.5 - 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.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				DFAS-Denver No relevant exception noted. **DFAS-Indianapolis** No relevant exception noted.
		1.6 - 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 after a specified period of time.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** No relevant exception noted.
		1.7 - When terminals are not in use, terminal rooms are locked, or the terminals are capable of being secured.	Inquired with appropriate personnel and observed facility to confirm that when terminals are not in use, terminal rooms are locked, or the terminals are capable of being secured.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<u>DFAS-Denver</u> We noted data entry terminals were not located in physically secure locations within locked rooms. The data entry terminals are located in an open space shared by non-payroll personnel who may be able to access sensitive payroll information. **<u>DFAS-Indianapolis</u>** Based on the procedures performed, the terminals are located within a physically secure building; however, terminal rooms are not located in physically secured locations within locked rooms and data entry terminals are connected to the system 24 hours a day, 7 days a week. The terminals are located in shared spaces with other agencies and non-payroll office personnel increasing the risk of unauthorized access to sensitive payroll information.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
2	Controls prevent unauthorized system access to DCPS data.	2.1 – The ability to view, modify, or transfer information contained in the payroll master files is restricted to authorized personnel. Each operator is required to have a completed and authorized authorization form before being granted access to the system. Authorization profiles over users limit what transactions data entry personnel can enter.	Inquired with appropriate personnel and inspected a sample of 45 System Access Authorization Request forms (i.e., SAAR) to confirm the following: • The payroll master file and output is restricted to authorized personnel; • Each operator is authorized before being granted access to the system; and Confirmed user profiles limit the type of transactions data entry personnel can enter into DCPS.	**<u>All Payroll Offices</u>** Of the 45 SAARs selected for testing, three employees were no longer DCPS users and were not active in the system; therefore, forms could not be provided for these users. Of the 42 non-payroll SAAR forms inspected, noted the following: • 1 of 42 forms indicated a user type which did not match the user type in the list of DCPS users by database; • 3 of 42 forms indicated authorization types which did not match the authorization type in the list of DCPS users by database; • 3 of 42 forms were missing the DCPS Security Awareness (WBT) completion date;

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				• 1 of 42 forms was missing the user's signature; • 1 of 42 forms was missing the supervisor's signature; • 9 of 42 forms were missing the date of the supervisor's signature; • 5 of 42 forms were missing the security manager's signature; and • 10 of 42 forms were missing the date of the security manager's signature. Of the 42 payroll SAAR forms inspected, noted the following: • 6 of 42 forms indicated a user type which did not match the user type in the list of DCPS users by database; • 3 of 42 forms indicated authorization types which did not match the authorization type

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				in the list of DCPS users by database; • One of 42 forms were 1 the DCPS Security Awareness (WBT) completion date; • 2 of 42 forms were missing the supervisor's signature; • 12 of 42 forms were missing the date of the supervisor's signature; • 2 of 42 forms were missing the security manager's signature; and • 4 of 42 forms were missing the date of the security manager's signature. Furthermore, we noted that for payroll office user testing, the forms that had user types which did not match the list of DCPS users by database are actually for non-payroll personnel who have payroll office access (based on the site activity code). The forms provided indicate that five of the six

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				individuals are human resources personnel (P) with view (V) access; the sixth individual is accounting personnel (V) with accounting technician (J) access. However, the six individuals were included in the list of DCPS Users by Database as N, V combinations; meaning that rather than inputting the user type/indicator code into DCPS as it appeared on the DISA 195-1 form, technicians entered these users with "N" user type/indicator codes with "V" authorization types; an authorization type which is correct for five of the six users.
		2.2 – Policies and procedures are documented to describe that 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.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** We identified a limitation within the DCPS system that prevents payroll technicians from adhering

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				to the guidance in the DCPS Security Guidelines Manual. We noted technicians input a code into DCPS that did not correspond with the codes indicated on the SAAR (see related results of testing in control activity 2.1). DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective. **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** No relevant exception noted.
		2.3 – On-line access logs are maintained by the System Management Office (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	This control activity is tested by GCC Control Activity 7.2. No relevant exception noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			the SMO, and the logs are reviewed regularly for unauthorized access attempts.	**DFAS-Pensacola** We noted that violations may have occurred during the audit period in which user(s) were attempting to access accounts for which they were not authorized. Adequate documentation was not available at the payroll office to allow us to investigate this issue further. DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective.
		2.4 – Remote terminal connections are secured and are connected via government issued computers.	Inquired with appropriate personnel and observed Telework Packages to confirm remote terminal connections are secured and are connected via government computers. Specifically, inspected the telework packages for each employee to confirm all employees completed the following documentation, and each document contained the required signatures:	**DFAS-Pensacola** 7 out of the 11 telework packages tested were incomplete, specifically: • 7 of 11 packages were missing a Telework Application; leaving only 4 Telework Applications for testing;

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			1. VPN Request Form; 2. TSO MOA; 3. Telework Application; 4. DFAS 1402, Safety Checklist; and 5. DFAS 1400, DFAS MOA.	• 3 of 11 packages were missing a DFAS 1402 (Safety Checklist); leaving only 8 DFAS 1402s for testing; and • 4 of 11 packages were missing a DFAS 1400 (Telecommuting Agreement); leaving only 7 DFAS 1400s for testing. All 11 packages contained a VPN User Access Request Form and a TSO MOA. No exceptions were noted with VPN request forms; all11 VPN request forms contained employee signatures. The following exceptions were noted with TSO MOA testing: • 5 of 11 TSO MOAs were missing employee signature dates; and • 3 of 11 TSO MOAs were missing supervisor signature dates.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				The following exceptions were noted with DFAS 1402 testing: • 2 of 8 were missing employee signatures and dates; and • 1 of 8 was missing employee signature date only. The following exceptions were noted with DFAS 1400 testing: • 4 of 7 were missing employee signatures; • 5 of 7 were missing employee signature dates; and • 3 of 7 were missing supervisor signatures and dates. DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<u>DFAS-Charleston</u> We confirmed that nine of nine teleworking employees were using Government-issued computers and connecting to DCPS through a VPN. However, we noted the following exceptions while testing the Telework packages: • 1 of 9 Property Passes was missing the property custodian's signature and employee's signature and date; • 2 of 9 DFAS 1402 forms were missing the employee signatures and dates; and 1 of 9 packages was missing a DFAS 1400 form (Telecommuting Agreement). Of the remaining eight DFAS 1400 forms inspected:

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				• 1 of 8 forms was missing a supervisor's signature and date. DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective. **DFAS-Denver** We were unable to test whether remote terminal connections are secured and are connected via Government-issued computers because Telework packages were not available for review. DFAS management indicated that once all Government equipment was returned to DFAS Denver, all Telework files were destroyed as part of the process to recall Telework personnel in April, 2007. DFAS management indicated the testing exception was caused by

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective. **<u>DFAS-Indianapolis</u>** DFAS personnel have remote access to DCPS using non-DoD-issued computers which is in violation of the DFAS Telework policy. DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective.
		2.5 – 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.	**<u>DFAS-Pensacola</u>** No relevant exception noted. **<u>DFAS-Charleston</u>** No relevant exception noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				DFAS-Denver No relevant exception noted. **DFAS-Indianapolis** See Control Activity 1.4 – DFAS-Indianapolis (above) for testing results. Exception Noted.
		2.6 – User IDs 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 IDs and passwords are required to gain access to the DCPS application.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** No relevant exception noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
3	Controls provide reasonable assurance that DCPS authorized users are restricted to access only areas needed to complete their assigned responsibilities and controls maintain segregation of duties.	3.1 – The detailed 592 payroll reconciliation shows all pertinent data describing the payroll (including total disbursements, Retirement, Thrift Savings Plan (TSP), Bonds, and other withholdings) and the related balances are reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS. All reconciling items are investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	Inquired with appropriate personnel and inspected a 100% sample of 26 592 reconciliations for each database to confirm: 1) The detailed payroll reconciliation shows pertinent data describing the payroll (including total disbursements, Retirement, TSP, Bonds, and other withholdings) and the related balances are reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS; 2) Each 592 reconciliation is approved by management prior to disbursement; and 3) Reconciling items are investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	**DFAS-Pensacola** *CP1 Database* Of the 26 592 reconciliation reports, we observed that one report did not have a certifying officer's signature. *ZKA Database* Of the 26 592 reconciliation reports, we observed that 2 of the 2812 Statements of Withholding were not signed and dated, and 3 of the 2812 Statements of Withholding were not dated. **DFAS-Charleston** *ZGT Database* Of the 26 592 reconciliation reports, we observed that one report was corrected by the preparer but not reconciled; 1 report did not balance even when a supplemental was prepared, and did not have the 592 preparer's signature; 3 reports were corrected but did not balance and did not have a

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				corresponding supplemental worksheet. Additionally, an inconsistency was confirmed in the DFAS Charleston Payroll Center's procedure for recording adjustments to the 592 when the report is initially out of balance or does not include all of the lines of accounting that are required for full reconciliation. **<u>DFAS-Denver</u>** No relevant exception noted. **<u>DFAS-Indianapolis</u>** *ZPV Database* Of the 26 592 reconciliation reports, 5 were processed by the Veterans Affairs, therefore, only 21 592 reports were tested. Of the 21 592 reconciliation reports inspected 2 withholding reports were not signed.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		3.2 – Summary payroll reports including OLQs of total disbursements, Retirement, Thrift Savings Plan (TSP), Bonds, and other withholdings are reviewed and approved by management prior to disbursement.	Inquired with appropriate personnel and inspected summary reports and OLQs reviewed and approved by management prior to disbursement.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** No relevant exception noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
4	Controls provide reasonable assurance that system and software changes are authorized, effectively and efficiently implemented, tested and documented. (General Computer controls only)	N/A as this is tested by the General Computer Controls.	N/A as this is tested by the General Computer Controls.	N/A

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
6	Controls include an enterprise wide security program to review and manage risks and ensure policies comply with laws and regulations.	6.1 – A Security Program has been prepared specific to payroll operations and is approved by management. The plan is regularly tested and updated to reflect the results of such tests.	Inquired with appropriate personnel to confirm a Security Program for payroll operations exists. Obtained and inspected the date of the plans and corroborated with management that these plans are current, contain up-to-date information, and are readily available to all relevant personnel. Inquired with management to confirm that the plans have been approved.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** We could not conduct testing for this control activity. The DFAS Indianapolis Payroll Office only started processing payroll in May 2007; therefore, an FFMIA annual certification has not yet been performed. Since this control activity had not been performed at this location during our period of testing, we can not conclude on the effectiveness of this control.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
7	Controls provide reasonable assurance that personnel and payroll data processed and stored at the DFAS and DISA (GCC) locations are valid, accurate, authorized, complete, [and] timely, support financial reporting requirements and provide sufficient audit trails.	7.1 – Policies and procedures are documented to describe that only valid and accurate changes are made to the payroll master files and payroll withholding tables.	Inquired with appropriate personnel and read policies and procedures to confirm that only valid changes are made to the payroll master files and payroll withholding tables.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** Exceptions noted. Please see testing performed in Control Activity 7.10. **DFAS-Indianapolis** No relevant exception noted.
		7.2 – Programmed validation and edit checks identify erroneous data.	Inquired with appropriate personnel and observed programmed validation and edit checks to confirm they identify erroneous data entered directly into DCPS.	**DFAS-Pensacola** No relevant exception noted.
		7.3 – The ability to view, modify, or transfer information contained in the payroll master files is restricted to authorized personnel.	Inquired with appropriate personnel and inspected haphazard sample of 45 System Access Authorization Request forms (i.e., SAARs) to confirm the master file is restricted to authorized personnel.	**All Payroll Offices** Of the 45 SAARs selected for testing, 3 employees were no longer DCPS users and were not active in the system; therefore,

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				forms could not be provided for these users. Of the 42 non-payroll SAAR forms inspected, noted the following: • 1 of 42 forms indicated a user type which did not match the user type in the list of DCPS users by database; • 3 of 42 forms indicated authorization types which did not match the authorization type in the list of DCPS users by database; • 3 of 42 forms were missing the DCPS Security Awareness (WBT) completion date; • 1 of 42 forms was missing the user's signature; • 1 of 42 forms was missing the supervisor's signature;

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				• 9 of 42 forms were missing the date of the supervisor’s signature; • Five of 42 forms were missing the security manager’s signature; and • 10 of 42 forms were missing the date of the security manager’s signature. Of the 42 payroll SAAR forms inspected, noted the following: • 6 of 42 forms indicated a user type which did not match the user type in the list of DCPS users by database; • 3 of 42 forms indicated authorization types which did not match the authorization type in the list of DCPS users by database; • 1 of 42 forms were missing the DCPS Security Awareness (WBT) completion

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				date; • 2 of 42 forms were missing the supervisor's signature; • 12 of 42 forms were missing the date of the supervisor's signature; • 2 of 42 forms were missing the security manager's signature; and • 4 of 42 forms were missing the date of the security manager's signature. Furthermore, we noted that for Payroll Office user testing, the forms that had user types which did not match the list of DCPS users by database are actually for Non-Payroll personnel who have Payroll Office access (based on the site activity code). The forms provided indicate that five of the six individuals are human resources personnel (P) with view (V) access; the sixth individual is accounting personnel (V)

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				with accounting technician (J) access. However, all six individuals were included in the list of DCPS users by database as N, V combinations; meaning that rather than inputting the user type/indicator code into DCPS as it appeared on the DISA 195-1 form, technicians entered these users with "N" user type/indicator codes with "V" authorization types; an authorization type which is correct for 5 of the 6 users.
		7.4 – Changes to the payroll withholding tables and master files are compared to authorized source documents by supervisory personnel to ensure that they were input accurately.	Inquired with appropriate personnel and observed the process of tax changes to the payroll withholding tables and master files being compared to authorized source documents by supervisory personnel to confirm that they were tested and approved. Inquired with appropriate personnel and observed the Imaging process to confirm that inputs are compared to authorized Imaging documents to confirm that they were input accurately.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** No relevant exception noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<u>DFAS-Indianapolis</u> No relevant exception noted.
		7.5 – Policies and procedures are documented to describe that changes made to the payroll master files and withholding tables are authorized, input, and processed timely.	Inquired with appropriate personnel and read policies and procedures to confirm that changes to the payroll master files and withholding tables are authorized, input, and processed timely.	**<u>DFAS-Pensacola</u>** No relevant exception noted.
		7.6 – Policies and procedures are documented to describe that changes made to the payroll master files and withholding tables are authorized, input, and processed timely.	Inquired with appropriate personnel and read policies and procedures to confirm that changes to the payroll master files and withholding tables are authorized, input, and processed timely.	**<u>DFAS-Charleston</u>** No relevant exception noted.
		7.7 – Policies and procedures are documented to describe that changes made to the payroll master files and withholding tables are authorized, input, and processed timely.	Inquired with appropriate personnel and read policies and procedures to confirm that changes to the payroll master files and withholding tables are authorized, input, and processed timely.	**<u>DFAS-Denver</u>** Exceptions noted. Please see testing performed in Control Activity 7.10.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		7.8 – Policies and procedures are documented to describe that changes made to the payroll master files and withholding tables are authorized, input, and processed timely.	Inquired with appropriate personnel and read policies and procedures to confirm that changes to the payroll master files and withholding tables are authorized, input, and processed timely.	**<u>DFAS-Indianapolis</u>** No relevant exception noted.
		7.9 – Changes to the payroll master file and withholding table data are logged in numerous reports and reviewed by supervisory personnel to ensure that all requested changes are processed timely.	Inquired with appropriate personnel and inspected reports to confirm that changes to the payroll master file and table data are logged and reviewed by supervisory personnel.	**<u>DFAS-Pensacola</u>** No relevant exception noted. **<u>DFAS-Charleston</u>** No relevant exception noted. **<u>DFAS-Denver</u>** No relevant exception noted. **<u>DFAS-Indianapolis</u>** No Relevant Exceptions Noted.
		7.10 – Requests to change the payroll master file data and withholding table are submitted on pre-numbered Remedy Tickets; the numerical sequence of the Remedy Tickets is accounted for to ensure that the requested changes are processed timely. Access to source documents is	Inquired with appropriate personnel and inspected a haphazard sample of 45 Remedy Tickets to confirm the requests: • are pre-numbered; • the sequence is accounted for so that the forms are accounted for timely; • access to the source documents is	**<u>DFAS-Pensacola</u>** Of the 45 remedy tickets inspected, 4 were not completed within the escalation timeframe prescribed by management.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		controlled; Key source documents require signatures from supervisory personnel.	controlled; and • key source documents require signatures from supervisory personnel.	DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective. **<u>DFAS-Charleston</u>** The numerical sequence of the remedy tickets was not continuous. Of the universe of remedy tickets inspected, there were 13 remedy tickets missing. **<u>DFAS-Denver</u>** Of the 45 remedy tickets inspected; 1 was not processed within the escalation timeframe prescribed by management. DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				prevent the control activity from meeting its related control objective. **DFAS-Indianapolis** No relevant exception noted.
		7.11 – Payroll master file data and withholding table data are edited and validated and errors identified on the Personnel Interface Invalid Report are corrected promptly.	Inquired with appropriate personnel and inspected a sample of 45 Personnel Interface Invalid Reports of erroneous transactions to confirm items are investigated and resolved timely.	**DFAS-Pensacola** Of the 45 Personnel Interface Invalid Reports selected for review, 16 could not be located. Of the 29 Personnel Interface Invalid Reports inspected: • 8 reports were missing the technician's signature on the report; • 8 reports were missing the date of when the report was annotated by the technician; and • 29 were inconsistently annotated with codes outlined in the SOP. We confirmed that the requirement for technicians to annotate every transaction did not take effect until May 27, 2007. One report

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				in the random sample fell after this date (June 18, 2007). We scanned this report and noted that the technician annotating this report failed to comply with the new requirement, and transactions were annotated inconsistently. None of the 29 reports provided and scanned contained sufficient detail to confirm resolution of all errors in the reports. **DFAS-Charleston** Of the 45 Personnel Interface Invalid Reports selected for review, no interface errors occurred for 9 of the reports selected. Of the 36 Personnel Interface Invalid Reports inspected, only 1 was not annotated correctly. Furthermore, evidence of supervisory review of Personnel Interface Invalid Reports could not be obtained for the sample selected in Control Activities 7.11/7.23.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				The Personnel Interface Invalid Reports SOP states a supervisor reviews 10% of the Payroll Technician's annotated reports on file. **DFAS-Denver** *OMA Database* Of the 45 Personnel Interface Invalid Reports inspected, 5 reports provided did not contain annotations by the payroll office technician for each line item that described the error correction method. *ZPA Database* Of the 45 Personnel Interface Invalid Reports selected, 1 report could not be located for review. **DFAS-Indianapolis** *ZPV Database* ZPV Personnel Interface Invalid Reports processing was performed at the Pensacola Payroll Office from August 20, 2006, through May 12, 2007. The Pensacola Payroll Office was unable to supply Personnel Interface

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				Invalid Reports documentation for August 20, 2006, through January 19, 2007; therefore, testing could not be conducted for this timeframe. Of the reports requested for the remaining audit period (26 reports in total), one could not be located. Of the 25 inspected, 15 were missing a date; 1 did not include a technician's signature; and 4 were not properly annotated.
		7.12 – Policies and procedures are documented to describe that 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.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** No relevant exception noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		7.13 – 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 management monitored payroll disbursement processing schedule.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** No relevant exception noted.
		7.14 – The detailed 592 payroll reconciliation shows all pertinent data describing the payroll (including total disbursements, Retirement, Thrift Savings Plan (TSP), bonds, and other withholdings) and the related balances are reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS. All reconciling items are investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	Inquired with appropriate personnel and inspected a 100% sample of 26 592 reconciliations for each database to confirm: 1) The detailed payroll reconciliation shows pertinent data describing the payroll (including total disbursements, Retirement, TSP, bonds, and other withholdings) and the related balances are reconciled, in the appropriate accounting period, to corresponding general ledger accounts within DCPS;	**DFAS-Pensacola** *CP1 Database* Of the 26 592 reconciliation reports, we observed that 1 report did not have a certifying officer's signature. *ZKA Database* Of the 26 592 reconciliation reports, we observed that 2 of the 2812 Statements of Withholding were not signed and dated,

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			2) Each 592 reconciliation is approved by management prior to disbursement; and 3) Reconciling items are investigated and cleared on a timely basis by supervisory personnel, prior to disbursement.	and 3 of the 2812 Statements of Withholding were not dated. **DFAS-Charleston** *ZGT Database* Of the 26 592 reconciliation reports, we observed that 1 report was corrected by the preparer but not reconciled; 1 report did not balance when a supplemental 592 was prepared, and it did not have the 592 preparer's signature; 3 reports were corrected but did not balance and did not have a corresponding supplemental worksheet. Additionally, an inconsistency was confirmed in the DFAS Charleston Payroll Center's procedure for recording adjustments to the 592 when the report is initially out of balance or does not include all of the lines of accounting that are required for full reconciliation.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				<u>DFAS-Denver</u> No relevant exception noted. **<u>DFAS-Indianapolis</u>** *ZPV Database* Of the 26 592 reconciliation reports, 5 were processed by the Veterans Affairs, therefore, only 21 592 reports were tested. Of the 21 592 reconciliation reports inspected, 2 withholding reports were not signed.
		7.15 – Summary payroll reports including OLQs of total disbursements, Retirement, Thrift Savings Plan (TSP), Bonds, and other withholdings are periodically reviewed by supervisory personnel for accuracy and ongoing pertinence of the payroll master file and withholding tables, and approved by management prior to disbursement.	Inquired with appropriate personnel, obtained and inspected summary payroll reports and OLQs to confirm the following: • Payroll master files and withholding tables are periodically reviewed by supervisory personnel for accuracy and ongoing pertinence; and • Reports are approved by management prior to disbursement.	**<u>DFAS-Pensacola</u>** No relevant exception noted. **<u>DFAS-Charleston</u>** No relevant exception noted. **<u>DFAS-Denver</u>** No relevant exception noted. **<u>DFAS-Indianapolis</u>** No relevant exception noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		7.16 – Policies and procedures are documented to describe that disbursed payroll (including compensation and withholding) is accurately calculated and recorded.	Inquired with appropriate personnel and read policies and procedures to confirm that disbursed payroll is accurately calculated and recorded.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** Exceptions noted. See testing performed in Control Activity 7.21.
		7.17 – DCPS performs limit and reasonableness checks on employee earnings.	Inquired with appropriate personnel and inspected a limit and reasonableness report to confirm reasonableness checks are performed on employee earnings.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** We noted that large payroll increases occurred in the pay periods ending March 17, 2007, and May 12, 2007, for the ZPD payroll database and the ZFR payroll database respectively. These large increases were for annual pay bonuses that were paid in the appropriate pay period. DFAS-Charleston

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				was unable to provide us documentation to confirm the reasons that were given for the large payroll increases. DCPS does not have a limit or reasonableness check requirement to identify variances at the total payroll level. **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** Confirmed the Less than $1 Greater than $5,000 Desk Guide did not have documented procedures requiring a supervisor to review 10% of the entries in the report, or the requirement to evidence the review with a signature or similar notation.
		7.18 – Policies and procedures are documented to describe that 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.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				DFAS-Denver No relevant exception noted. **DFAS-Indianapolis** No relevant exception noted.
		7.19 – Supervisory personnel periodically review listings, such as the Personnel/Payroll Reconciliation Report, of current employees within each user organization and notify the corresponding user organization's personnel department of necessary changes.	Inquired with appropriate personnel and inspected the Personnel/Payroll Reconciliation Report to confirm it is sent to management for review of employee listings personnel department notified of changes. Obtained and inspected a sample of 45 Personnel/Payroll Reconciliation Reports, along with the corresponding supervisor document log, to confirm items that require resolution are investigated and resolved by the appropriate personnel. Additionally, inspected the supervisor document log to confirm the quarterly Pay Personnel Reports are logged and both supervisor and personnel signatures are captured.	**DFAS-Pensacola** Noted the Pensacola Payroll Office does not send a letter of completion signed by the supervisor to the personnel offices as documented in the SOP. Of the 45 Personnel/Payroll Reconciliation Reports inspected, 1 report for Thrift Savings Plan (TSP) changes, which is handled by the Support Services Branch, could not be located. Additionally, we identified that reports that go to that branch are not maintained with a cover sheet as required by the SOP. Four reports were not completed within 10 working days as required

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				by the SOP. **DFAS-Charleston** DFAS-Charleston did not receive any Personnel/Payroll Reconciliation Reports for 3 of the 4 quarters of our audit period and received only 4 reports for another quarter. The most recent quarter reports were supplied; however, we were unable to test as the reconciliation process was not yet complete. Therefore, testing could not be performed. Furthermore, for the reports that were supplied, noted the Charleston Payroll Office does not create adequate cover sheets for the Personnel/Payroll Reports as required by the DFAS entity-wide Personnel/Payroll Reconciliation SOP.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				DFAS-Denver DFAS Denver does not retain Personnel/Payroll Reconciliation packages (i.e., coversheet, report) as required by the DFAS Pay Personnel Reconciliation SOP; therefore, testing could not be performed. **DFAS-Indianapolis** We could not conduct testing for this control activity. The Indianapolis Payroll Office has not yet performed reconciliation between the personnel system, Defense Civilian Personnel Data System (DCPDS), and DCPS as it has only processed 3 payrolls within the audit period. Since this control activity had not been performed at this location during our period of testing, we can not conclude on the effectiveness of this control.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		7.20 – Only authorized personnel have the ability to disburse payroll.	Inquired with the appropriate personnel, observed the disbursement of payroll, and inspected a sample of 45 DCPS user profiles to confirm that only authorized personnel have the ability to disburse payroll.	**All Payroll Offices** Of the 56 SAAR forms inspected for persons with the ability to disburse payroll, 1 was missing a supervisor signature.
		7.21 – Policies and procedures are documented to describe that controls provide reasonable assurance of the integrity and reliability of DCPS data for financial reporting purposes.	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.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** A policy and/or procedure does not exist that requires the 592 reconciler to identify an increase in total payroll or to document and include the reason for increase in the 592 file when one occurs (see additional results of testing in Control Activity 7.19). **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** Policies and procedures for reconciling the 592 reports have not been developed and documented.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		7.22 – Payroll transactions at the end of a payroll cycle are reconciled by supervisory personnel to ensure complete and consistent recording in the appropriate accounting period.	Inquired with appropriate personnel and inspected a 100% sample of 26 592 payroll reconciliations at the end of a payroll cycle to confirm they are reconciled to confirm complete and consistent recording in the appropriate accounting period.	**<u>DFAS-Pensacola</u>** *CP1 Database* Of the 26 592 reconciliation reports, we observed that 1 report did not have a certifying officer's signature. *ZKA Database* Of the 26 592 reconciliation reports, we observed that 2 of the 2812 Statements of Withholding were not signed and dated, and 3 of the 2812 Statements of Withholding were not dated. **<u>DFAS-Charleston</u>** *ZGT Database* Of the 26 592 reconciliation reports, we observed that 1 report was corrected by the preparer but not reconciled; 1 report did not balance when a supplemental was prepared, and it did not have the 592 preparer's signature; 3 reports were corrected but did not balance and did not have a corresponding

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				supplemental worksheet. Additionally, an inconsistency was confirmed in the DFAS Charleston Payroll Center's procedure for recording adjustments to the 592 when the report is initially out of balance or does not include all of the lines of accounting that are required for full reconciliation. **<u>DFAS-Denver</u>** No relevant exception noted. **<u>DFAS-Indianapolis</u>** *ZPV Database* Of the 26 592 reconciliation reports requested, 5 pay periods were processed and reconciled by the Veterans Affairs on their own behalf, therefore, only 21 592 reports were considered in scope and tested. Of the 21 592 reconciliation reports inspected 2 withholding reports were not signed.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		7.23 – Error reports, such as the Personnel Interface Invalid Report, and error warnings show rejected transactions with error messages that have clear understandable corrective actions for each type of error. 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, date and time the transaction was processed and the error identified, and the identity of the user who originated the transaction. Users review the Personnel Interface Invalid Reports for data accuracy, validity, and completeness. A control group is responsible for controlling and monitoring rejected transactions included on the Personnel Interface Invalid Report.	Inquired with appropriate personnel and obtained a sample of 45 Personnel Interface Invalid Reports to confirm the following: • the reports show rejected transactions with error messages that have clear understandable corrective actions for each type of error; • 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, date and time the transaction was processed, the error identified, and the identity of the user who originated the transaction; • users review output for data accuracy, validity, and completeness; and • the report is used for controlling and monitoring rejected transactions.	**DFAS-Pensacola** Of the 45 Personnel Interface Invalid Reports selected for review, 16 could not be located. Of the 29 Personnel Interface Invalid Reports inspected: • 8 reports were missing the technician's signature on the report; • 8 reports were missing the date of when the report was annotated by the technician; and • 29 were inconsistently annotated with codes outlined in the SOP. We confirmed that the requirement for technicians to annotate every transaction did not take effect until May 27, 2007. One report in the random sample fell after this date (June 18, 2007). We scanned this report and noted that the technician annotating this report failed to comply with the new requirement and transactions were

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				annotated inconsistently. All 29 reports did not include the technician's annotation for each line item to confirm resolution of all errors in the reports. **DFAS-Charleston** Of the 45 Personnel Interface Invalid Reports selected for review, no interface errors occurred for 9 of the reports selected. Of the 36 Personnel Interface Invalid Reports inspected, 1 was not annotated correctly. Furthermore, evidence of supervisory review of Personnel Interface Invalid Reports (PIIR) could not be obtained for the sample selected in Control Activities 7.11/7.23. The PIIR SOP states a supervisor reviews 10% of the Payroll Technician's annotated reports on file. **DFAS-Denver** *OMA Database* Of the 45 Personnel Interface Invalid Reports

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				inspected, 5 did not contain annotations by the payroll office technician for each line item that described the error correction method. *ZPA Database* Of the 45 Personnel Interface Invalid Reports inspected, 1 could not be located for review. **DFAS-Indianapolis** *ZPV Database* ZPV PIIR processing was performed at the Pensacola Payroll Office from August 20, 2006 through May 12, 2007. The Pensacola Payroll Office was unable to supply PIIR documentation for August 20, 2006 through January 19, 2007; therefore, testing could not be conducted for this timeframe. Of the reports requested for the remaining period of the audit period (26 reports in total), 1 could not be located. Of the 25 inspected, 15 reports were missing a date, 1 did not

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				have a technician's signature, and 4 were not properly annotated.
		7.24 – Policies and procedures are documented to describe that capabilities exist for fiscal year-end, leave-year-end and calendar year-end processing and forfeitures in accordance with established 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. Obtained and inspected Payroll Quality Review (PQR) reports to confirm checklists are followed and payroll steps have been performed.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** We could not conduct testing for this control activity. DFAS Indianapolis has not performed year-end processing; therefore, no procedures were available for the audit period. Since this control activity had not been performed at this location during our period of testing, we can

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
				not conclude on the effectiveness of this control.
		7.25 – Payroll withholding table data is periodically reviewed by supervisory personnel 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.	**DFAS-Pensacola** No relevant exception noted.
		7.26 – The data processing control group has a schedule by application that shows when outputs should be completed, when they need to be distributed, who the recipients are, and the copies needed; reviews output products for general acceptability; and reconciles control information to determine completeness of processing.	Inquired with appropriate personnel and inspected the schedules used by the data processing group, to confirm they: • 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; • review output products for general acceptability; and reconcile control information to determine completeness of processing.	**DFAS-Pensacola** No relevant exception noted.

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
		7.27 – Policies and procedures are documented to describe that current- or prior-period adjustments to employee's pay, including employee debt, tax deduction, or deductions not 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 deduction, or deductions not taken, are reported, reconciled and approved.	**DFAS-Pensacola** No relevant exception noted. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** No relevant exception noted.
		7.28 – Policies and procedures are documented to describe that 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. Obtained and inspected a sample of 45 HHS transactions input to DCPS to confirm transactions from interfacing systems are subjected to the payroll system edits, validations, and error-correction procedures. Additionally, inspected associated reports (i.e.,	**DFAS-Pensacola** The DCPS SYSOUT SOP is one page in length and does not describe all activities performed for investigating and correcting erroneous data. The DCPS SYSOUT is an online report that contains mainframe processing results, including run-to-

No.	Control Objective	Control Activities	Tests Performed	Results of Testing
			MyPay Invalid Reports and MER Add/Change/Delete Reports) to confirm they are reviewed by appropriate personnel, and any exceptions identified are investigated and resolved.	run balancing and system error messages, if applicable. DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective. **DFAS-Charleston** No relevant exception noted. **DFAS-Denver** No relevant exception noted. **DFAS-Indianapolis** No relevant exception noted.
		7.29 – The system provides an audit trail of all transactions processed, transaction errors, error descriptions, and error correction procedures. Audit trails are reviewed by supervisory personnel and erroneous data are captured, reported, investigated, and corrected.	Inquired with appropriate personnel and inspected audit trails of transactions to confirm that erroneous transactions are reviewed by supervisory personnel, captured, reported, investigated, and corrected.	**DFAS-Pensacola** No relevant exception noted.

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

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

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
1	**Security Programs Effectiveness Monitoring**			
1.1	Controls provide reasonable assurance that the security program effectiveness is monitored and changes are made as needed.	1.1.1 DISA DECC Mechanicsburg & DFAS Saufley Field DoD and DFAS policy both direct annual Information Assurance (IA) review.	DISA DECC Mechanicsburg & DFAS Saufley Field Interviewed the Security Officer to obtain an understanding of how management assessed the appropriateness of the security policies and compliance with them.	No relevant exception noted.
1.2	Management monitors compliance with policies and procedures.	1.2.1 DISA DECC Mechanicsburg The Director's Policy Letters (DPLs) and Standard Operating Procedures (SOP) are reviewed and updated. Security Readiness Review (SRR) is conducted at least every 3 years.	DISA DECC Mechanicsburg 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.	No relevant exception noted.
1.3	Corrective actions are effectively implemented.	1.3.1 DISA DECC Mechanicsburg The Vulnerability Management System (VMS) 6.0 is used to track the status of outstanding Information Assurance Vulnerability Alerts (IAVAs) and the status of STIG findings from the Security Readiness Review (SRR) process. DECC Mechanicsburg management is responsible for tracking and closing	DISA DECC Mechanicsburg Observed the SRR process to confirm that corrective actions are effectively implemented for identified SRR findings. Selected a sample of SRRs and inspected the VMS reports to confirm findings identified by the SRR process have been addressed.	No relevant exception noted

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		all IAVA's and STIG findings that resulted from the SRR process. 1.3.2 DFAS Saufley Field Remediation plans detail corrective actions in response to findings identified in audits of DCPS or DFAS. Management has approved the remediation plan and monitors progress of the plan.	Requested prior audit reports or reviews and confirmed remediation had occurred for the findings and recommendations presented within. DFAS Saufley Field Requested prior audit reports or reviews and confirmed remediation has occurred for the findings and recommendations presented within the reports. Requested remediation plans intended to address previous findings to confirm remediation had been initiated.	

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
2	**Risk Assessment**			
2.1	Risk assessments are performed according to current Federal and DoD requirements.	2.1.1 DISA DECC Mechanicsburg & DFAS Saufley Field DoD and DFAS policy both direct an annual IA review.	DISA DECC Mechanicsburg Inquired with the Information System Security Officer (ISSO) and related security personnel and inquired how often the risk assessment process occurs. Observed the SRR process and confirmed how often it occurs and that deficiencies and corrective actions are tracked. Selected a sample of SRRs performed to inspect the Vulnerability Management System (VMS) reports to confirm findings identified by the SRR process have been addressed. DFAS Saufley Field Inquired with the ISSO and related security personnel and inquired how often the risk assessment process occurs. Inspected the lasted Risk Assessment, which should be included with the System Security Authorization Agreement (SSAA) to confirm that risks are periodically assessed.	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
3	**Site Security Plans**			
3.1	Site security plans are documented, approved, and are current.	3.1.1 DFAS Saufley Field DoD and DFAS policy both direct annual IA review. Review appropriate generated documentation to ensure that these processes are accomplished.	DFAS Saufley Field Inspected the DCPS SSAA to confirm it has been documented, kept current and appropriately approved by management. Inspected DCPS Systems Security Policy, Security Requirements, and Certification Test and Evaluation Plan and Procedures to confirm that each has been updated.	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
4	**Security Management Structure**			
4.1	A security management structure has been established with DCPS.	4.1.1 DFAS Saufley Field The DCPS SSAA describes the IA operations of the DoD information system and clearly delineates IA responsibilities and expected behavior of all personnel.	DFAS Saufley Field Confirmed through inquiry that a management structure had been established. Obtained and inspected security management organization chart. Requested one position description for each function listed on the organization chart to confirm that positions were established in writing. Inspected the SSAA for the security management structure. Confirmed each position function is outlined in the SSAA.	No relevant exception noted.
4.2	Information security responsibilities are clearly assigned.	4.2.1 DISA DECC Mechanicsburg & DFAS Saufley Field The DISA SMC-ME SSAA and the DCPS SSAA both describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel.	DISA DECC Mechanicsburg Inspected signed rules of behavior statements for the DISA personnel with access to DCPS and the underlying operating system. DFAS Saufley Field Inspected the SSAA for the security management responsibilities. Confirmed that each position is outlined in the SSAA is filled by personnel and the personnel understand their duties.	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			Inspected signed rules of behavior statements for the DFAS personnel with access to DCPS.	

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
4.3	Employees are aware of security policies.	4.3.2 DFAS Saufley Field Ongoing security awareness programs that include initial training and periodic refresher training.	DFAS Saufley Field Inspected the Security Awareness Training materials. Obtained a list of employees who have access to DCPS. Selected a sample of employees who have DCPS access and inspected their training files to confirm the completion of the necessary security training and a signoff. Obtained evidence that management has active security awareness programs in place (i.e. electronic mail files, or other policy distribution mechanisms) that proactively emphasize the security policies to data owners and users.	No relevant exception noted.
4.4	A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place.	4.4.1 DISA DECC Mechanicsburg Vulnerabilities are tracked in the Vulnerability Management System (VMS) database. Prior to connection to the network, the SA must run a VS08 report detailing Information Assurance Vulnerability Management (IAVM) notices for the asset's operating system. All IAVM notices must be mitigated and applicable patches loaded prior to connecting the asset to the network. Once all checklists have been applied from the Security Technical Information Guide (STIG) and the patches from the vulnerability alerts have been installed, a self assessment	DISA DECC Mechanicsburg Obtained the VMS reports for the audit period for DCPS and confirmed vulnerabilities are being tracked and resolved in a timely manner.	No relevant exception noted.

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

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
5	**Personnel Policies**			
5.1	Employee (Government or contractor) background investigations, hiring, transferring, and termination policies address security and are in compliance with DoD Instruction 8500.02.	DFAS Saufley Field The DCPS SSAA requires system users to be subjected to various levels of Personnel Security Investigations (PSI's) based on the level of access or privileges they have within the systems. The higher the level of access, the more stringent the required investigation becomes. As a minimum, all DFAS DCPS personnel/employees (military, civilian or contractors) will have a favorably completed NAC.	DFAS Saufley Field Requested, obtained, and inspected the policies and procedures for gaining access to sensitive information. Obtained a listing of all personnel associated with DCPS. Selected a sample of DCPS users and obtained the SAAR Form 2875 for each. Confirmed that each SAAR Form 2875 details the user's justification for access, security clearance level, and the proper approvals.	**DFAS Saufley Field** For 2 of the 45 sampled DCPS users from DFAS TSO PE, the Justification for Access (block 13) on the DD2875 Access Request Form was not complete. For 4 of the 45 sampled DCPS users from DFAS TSO PE, the Justification for Access (block 13) on the DD2875 Access Request Form was not specific to job duties. DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
5.2	Job descriptions for Government employees have been documented, and employees understand their duties and responsibilities.	5.2.1 DISA DECC Mechanicsburg and DFAS Saufley Field Developed position descriptions for distinct system support positions.	DISA DECC Mechanicsburg Inspected the job descriptions for the applicable types of personnel. DFAS Saufley Field Inspected the job descriptions for the applicable types of personnel listed in control objective # 5.1.	No relevant exception noted.
		5.2.2 DISA DECC Mechanicsburg and DFAS Saufley Field Position descriptions are available and Performance Plans are provided to assist employees in understanding their roles and responsibilities according to their assigned duties.	DISA DECC Mechanicsburg Selected a sample of employees and confirmed through inquiry that they understood their duties and responsibilities. Observed documentation to confirm that employees have signed position descriptions. DFAS Saufley Field Selected a sample of employees and confirmed through inquiry that they understood their duties and responsibilities. Observed documentation to confirm that employees have signed their performance plans.	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		5.2.3 DFAS Saufley Field All DFAS personnel are required to complete initial and periodic IA training. This training helps the employee understand the importance of their roles and responsibilities.	DFAS Saufley Field Inspected the hiring, transfer, termination and performance policies to confirm they are documented and address security. Confirmed though inquiry that debriefs are conducted when employees are terminated and that a HR Checklist is used to note the collection of DFAS property. Confirmed through observation that an email is sent to the System Administrator to request that system access be removed for a terminated employee.	No relevant exception noted.
5.3	Employee (Government or contractor) is adequately trained and possess the required skills.	5.3.1 DISA Mechanicsburg & DFAS Saufley Field A program is implemented to ensure that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA- related plans such as incident response, configuration management and COOP or disaster recovery.	DISA DECC Mechanicsburg Confirmed through inquiry that a training program has been established. Requested documentation to confirm the existence of this training program. (examples can include: individual training plans, job specific training plans, policy for requirements of training) If training is conducted in-house, inspected the training materials to confirm that they provided personnel with adequate training and expertise. Selected a sample of employees who have access to DCPS and inspected their training records to confirm specific job function training is occurring DFAS Saufley Field Confirmed through inquiry that a training program has been established	**DISA DECC Mechanicsburg** For 2 of the 22 DISA DECC Mechanicsburg employees selected in the sample, the employee's Individual Development Plans do not have job related training scheduled. Specifically, only 1 training session had been scheduled and it was unrelated to the employee's job function. For 1 of the 22 DISA DECC Mechanicsburg employees selected in the sample, the

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			Requested documentation to confirm the existence of this training program. (examples can include: individual training plans, job specific training plans, policy for requirements of training) If training is conducted in-house, inspected the training materials to confirm that they provided personnel with adequate training and expertise and that they are up to date. Selected a sample of employees who have access to DCPS and inspected their training records to confirm specific job function training is occurring.	employee's Individual Development Plan does not have any training scheduled. DISA management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective. **DFAS Saufley Field** No relevant exception noted.

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

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		DFAS Saufley Field DFAS management has identified DCPS resources supporting critical operations based on the nature and impact of the disaster. The resources are included in the DISA SMC ME Business Continuity Plan as prescribed in the SLA between DISA and DFAS.	management. DFAS Saufley Field Corroborated with key personnel that identification of resources supporting critical operations is based on the nature and impact of the disaster. Obtained and inspected the business continuity plan and confirmed that supporting critical operations are identified, emergency priorities are established, and they were approved by management.	
6.2	DFAS has classified all DFAS-owned assets according to criticality and sensitivity.	6.2.1 DFAS Saufley Field Management has classified DCPS according to appropriate MAC level standards.	DFAS Saufley Field 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 has been assigned to DCPS. Inspected the DCPS Service Level Agreement (SLA) between DFAS and DISA to determine the classification of DCPS communicated to DISA.	**DFAS Saufley Field** DFAS does not have MOAs in place for 4 of the 81 DCPS interfaces.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
6.3	Data management and the disposition and sharing of data requirements are identified in the SLAs.	6.3.1 DFAS Saufley Field Documented policies and procedures are in the DCPS SSAA that governs the sharing of data.	DFAS Saufley Field Inspected documents authorizing file sharing and file sharing agreements and confirmed the owners approve the sharing of data. In many cases these documents are called a Memorandum of Understanding (MOU) or SLA. 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 has been assigned to DCPS. Inquired with data owners and confirmed that an MOU has been developed and is in place for each DCPS interface.	**DFAS Saufley Field** DFAS does not have MOAs in place for 4 of the 81 DCPS interfaces.
6.4	DCPS has logical controls over data files and software programs.	6.4.1 DFAS Saufley Field The System Access Authorization Request (SAAR) DD-2875 form is used to identify authorized users and control their access.	DFAS Saufley Field Requested a complete DCPS user list. Selected a sample of users from the list and inspected their user access request forms for existence and management approval. Observed the application to confirm that users must possess a valid User ID and Password to gain access to the system. Interviewed owners and observed supporting documentation to confirm that inappropriate access is removed in a timely manner. Interviewed security managers and	**DFAS Saufley Field** DCPS does not use complex password configuration. In addition, DCPS does not require at least four characters be changed when a new password is created. Two of the 20 terminated DFAS Saufley Field employees and contractors were not

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			confirmed that supporting documentation was provided to them. Obtained a representative sample of profile changes and activity logs and confirmed that management reviewed the changes and logs. Obtained a list of recently terminated employees from personnel. Selected a representative sample of terminated employees and confirmed that system access was promptly terminated.	removed from DCPS within 24 hours of the user deactivation request sent in the personnel action email by Human Resources.
		6.4.2 DISA DECC Mechanicsburg The DISA System Support Office (SSO), a unit independent of SMC operations, is responsible for maintaining the system libraries however SMC Operations performs the library installation. Access to system libraries is restricted to authorized individuals including system programmers at SSO and SMC-ME.	DISA DECC Mechanicsburg Confirmed through inquiry and inspection of the root access users for the DCPS servers, that the access restrictions have been established around the data files and software programs. Inspected the access logs and corroborated with management that the access logs are reviewed for inappropriate access and that system libraries were managed and maintained to protect privileged programs.	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
7	**User Account Management**			
7.1	Authorized owners and their access rights are identified for DISA/DFAS-owned assets Access authorizations are appropriately limited.	7.1.1 DISA DECC Mechanicsburg & DFAS Saufley Field User accounts are suspended after 30 days of no activity, (60 days for TSO and Payroll offices) and removed after 90 days. Accounts are approved by IA Officers.	DISA DECC Mechanicsburg Inspected the policies and procedures for restricting access to the systems software to confirm that they were up-to-date. Obtained a list from the Discretionary Access Control (DAC) of individuals who had direct access to the system software and selected a sample of users with direct access. For each user selected, confirmed with key management personnel that these users were authorized to have this access. Inquired with key management that suspension and termination of access is performed according to the policies and procedures. Interviewed owners and observed supporting documentation to confirm that inappropriate access is removed in a timely manner. Obtained a list of recently terminated employees from personnel. Selected a representative sample of terminated employees and confirmed that system access was promptly terminated. DFAS Saufley Field Inspected the policies and procedures for	**DISA DECC Mechanicsburg** For 1 of the 45 sampled DCPS users from DISA DECC Mechanicsburg, the Justification for Access (block 13) on the DD2875 Access Request Form was not complete. For 3 of the 45 sampled DCPS users from DISA DECC Mechanicsburg, the Justification for Access (block 13) on the DD2875 Access Request Form was not specific to job duties. DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			restricting access to the DCPS application software to confirm that they were up-to-date. Obtained a list from the DAC of individuals who had direct access to the DCPS application software and selected a sample of users with direct access. For each user selected, confirmed with key management personnel that these users were authorized to have this access. Inquired with key management that suspension and termination of access is performed according to the policies and procedures. Interviewed owners and observed supporting documentation to confirm that inappropriate access is removed in a timely manner. Obtained a list of recently terminated employees from personnel. Selected a representative sample of terminated employees and confirmed that system access was promptly terminated.	**DFAS Saufley Field** For 2 of the 45 sampled DCPS users from DFAS Saufley Field, the Justification for Access (block 13) on the DD2875 Access Request Form was not complete. For 4 of the 45 sampled DCPS users from DFAS Saufley Field, the Justification for Access (block 13) on the DD2875 Access Request Form was not specific to job duties. One of the 45 sampled DCPS users from DFAS Saufley Field did not check the box indicating they received IA Training and Awareness Certification on the DD2875 Access Request Form. Two of the 20 terminated DFAS Saufley Field employees and contractors appear to not have been removed

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
				from DCPS within 24 hours of the user deactivation request sent in the personnel action email by Human Resources. DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective.
7.2	IAOs or SAs periodically review authorization listings to determine appropriateness. Policies and techniques have been implemented for using and monitoring use of system utilities.	7.2.1 DISA DECC Mechanicsburg Access to the system software is administered based on roles.	DISA DECC Mechanicsburg Inquired with key Mechanicsburg personnel to confirm how root and or privileged access is administered. Obtained the list of individuals with root and or privileged access. Inquired with Management that root and privileged access is appropriate and that the use of these accounts is logged. Inspected a sample of the audit logs from the DCPS servers to confirm that key personnel review the logs on a regular basis and that any issues noted are documented and researched.	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
7.3	Emergency and temporary access is controlled.	7.3.1 DISA DECC Mechanicsburg & DFAS Saufley Field Emergency and temporary access authorizations are controlled in accordance with DoD 5200.1-R; DoD 5200.2-R; DoDD 8500.1; and DoDI 8500.2. Accounts are approved by the IA officers.	DISA DECC Mechanicsburg Inspected the emergency and temporary access policy. Selected a sample of emergency and temporary access and • confirmed that the authorization was approved and that access was closed in a timely manner; • confirmed that the emergency and temporary access list is periodically reviewed; and • confirmed that temporary access authorizations were established for least privileged need-to-know access. DFAS Saufley Field Inspected the emergency and temporary access policy. Selected a sample of emergency and temporary access and: • confirmed that the authorization was approved and that access was closed in a timely manner; • confirmed that the emergency and temporary access list is periodically reviewed; and • confirmed that temporary access authorizations were established	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
			for least privileged need-to-know access.	
7.4	Group authenticators for application or network access may be used only in conjunction with an individual authenticator	7.4.1 DFAS Saufley Field Group authenticators are not used for DCPS or network access. Upon initial system login, a user's actions are tracked based on their unique user account.	DFAS Saufley Field Confirmed through inquiry if group authenticators for application and network are used. Inquired to understand the reason behind the usage of group authenticators. Inquired if users are authenticated individually prior to the use of a group authenticator. Confirmed through observation that group authentication is used by the operations group; however, mitigation controls are in place.	**DFAS Saufley Field** There are no formal Standard Operating Procedures for the review of the Operations Job Logs.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
8	**Physical Security**			
8.2	Building, administration, and computer facility physical controls have been implemented.	DFAS Saufley Field DFAS facilities at DFAS Saufley Field have implemented adequate physical security controls in accordance with DODI 8500.2. Physical access points are guarded or alarmed 24 hours a day. The Random Anti-Terrorism Measures (RAM) process is in place	DFAS Saufley Field Inquired with facility management as to the physical security controls in place. Confirmed through observation that these controls are in place. Obtained results of most recent facility penetration testing and confirmed that management reviewed the results of the test.	**DFAS Saufley Field** No relevant exception noted

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		that includes periodic, unannounced attempts to penetrate DFAS facilities. Only authorized personnel with appropriate access approval are granted physical access.		
8.3	Visitors are controlled.	8.3.2 DFAS Saufley Field All visitors must sign in and out on the visitor control log located in the main lobby. The DCPS SSAA requires all non-cleared personnel to be escorted at all times while inside the building.	DFAS Saufley Field Inspected the visitor policy and procedure to confirm it is documented. Confirmed through inquiry that all visitors are controlled. Confirmed through inquiry and observation that visitor access to DoD information was determined by both its classification and user need-to-know. Obtained the visitor check in log for a sample of normal business days. Confirmed the log has been completed according to the visitor policies and procedures.	**DFAS Saufley Field** Visitor log policy at DFAS Saufley Field is not consistently followed. For 1 day, a Point of Contact for an entry was missing, and for another day a visitor organization was missing for an entry. DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
9	**Logical Access**			
9.1	Access settings have been implemented in accordance with the access authorizations established by the resource owners.	9.1.1 DISA DECC Mechanicsburg Access settings have been implemented in accordance with the access authorizations established by signature authority of resource owner on Form DD2875 and in accordance with DoDD 8500.1; DoDI 8500.2 and STIGs. 9.1.2 DFAS Saufley Field The TSO assigns security profiles to each userid based on need to know as demonstrated by an approved Form DD2875, request for system access. TSO PE Database Administrator also assigns security profiles to development users through the Integrated Database Management System (IDMS) which restricts access to program libraries and databases.	DISA DECC Mechanicsburg Obtained a sample of users with access to DCPS LPAR and obtained the SAAR Form DD2875 for the sampled personnel. Confirmed that each Form 2875 details the user's justification for access, security clearance level, and that each Form 2875 is properly approved. DFAS Saufley Field Observed the DCPS system to confirm that each user account was assigned a Security Profile that restricts access by module or program. Requested a complete DCPS user list. Selected a sample of users from the list and inspected heir Form DD2875s that detail the user's justification for access, security clearance level and inspect for existence and approval by management.	**DISA DECC Mechanicsburg** For 1 of the 45 sampled DCPS users from DISA DECC Mechanicsburg, the Justification for Access (block 13) on the DD2875 Access Request Form was not complete. For 3 of the 45 sampled DCPS users from DISA DECC Mechanicsburg, the Justification for Access (block 13) on the DD2875 Access Request Form was not specific to job duties. DISA DECC Mechanicsburg management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
				<u>DFAS Saufley Field</u> For 2 of the 45 sampled DCPS users from DFAS Saufley Field, the Justification for Access (block 13) on the DD2875 Access Request Form was not complete. For 4 of the 45 sampled DCPS users from DFAS Saufley Field, the Justification for Access (block 13) on the DD2875 Access Request Form was not specific to job duties. One of the 45 sampled DCPS users from DFAS Saufley Field did not check the box indicating they received IA Training and Awareness Certification on the DD2875 Access Request Form. Two of the 20 terminated DFAS Saufley Field employees and contractors appear to

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
				not have been removed from DCPS within 24 hours of the user deactivation request sent in the personnel action email by Human Resources. DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective.
9.2	Passwords, tokens, or other devices are used to identify and authenticate users.	9.2.1 DFAS Saufley Field User IDs and passwords are configured according to DoD standards.	DFAS Saufley Field Observed that each user account was assigned a Security Profile that restricted access by module and program. Observed the DCPS application to confirm that users needed a valid User ID and password to gain access to the system. Inspected system parameters to make certain that the system requires a User ID and password.	**DFAS Saufley Field** DCPS does not use complex password configuration. ACF2 does support complex passwords; however, DISA and DFAS are in the process of transitioning the security configuration for MZF to allow the use of complex passwords. In addition, DCPS does not require that at least four

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
				characters be changed when a new password is created.
		9.2.2 DISA DECC Mechanicsburg Multiple layers of access controls are used including; Common Access Card (CAC) and personal identification number, DCPS user ID and password, and an RSA SecurID for Database Administration, Configuration Management, Security, and Tech Support.	DISA DECC Mechanicsburg Confirmed through inquiry and observation that passwords are used to authenticate users. Inspected system parameters to make certain that the system requires a User ID and password. Inspected the Security Account Creation Guide to confirm that authentication devices are in compliance with DoD standards.	**DISA DECC Mechanicsburg** Currently ACF2 password parameters are not configured to require the use of special characters. ACF2 is not configured to require users to change at least four characters of their previously used passwords.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
10	**Network and Telecommunications**			
10.1	Telecommunication defense capabilities are implemented. Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography.	10.1.1 DISA DECC Mechanicsburg SMC ME is in the process of encrypting all data streams to the FIPS-140-2 standard	DISA DECC Mechanicsburg Inquired with security personnel if DCPS data are transmitted through a commercial or wireless network. Inquired with security personnel to confirm that NIST cryptography was used to protect information when the information transmitted over commercial or wireless networks.	No relevant exception noted.
10.4	Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures is planned, scheduled, and conducted.	10.4.1 DISA DECC Mechanicsburg DISA SMC ME performs monthly scans to check for any DCPS network vulnerabilities. DCPS system and hardware are reviewed through periodic SRR reviews that are conducted by FSO on the DCPS mainframe domain.	DISA DECC Mechanicsburg Confirmed through inquiry that conformance testing are performed that include periodic, unannounced, in-depth monitoring and provided for specific penetration testing to confirm compliance with vulnerability mitigation procedures was planned, scheduled, and conducted. Obtained and inspected documentation produced from this conformance testing to confirm vulnerability scans were completed.	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
12	**Access Monitoring**			
12.1	Audit trails are maintained.	12.1.1 DISA DECC Mechanicsburg and DFAS Saufley Field A security audit trail is implemented for each system that documents the identity of each person/device having access to a system, the time of that access, user activity, and any actions which attempt to change security levels or privileges established for the user. The management of the audit trail is maintained by DISA.	DISA DECC Mechanicsburg Confirmed through inquiry that audit trails are implemented for the MZF LPAR. Inspected the audit trails available and confirmed what information is being logged. Confirmed through inquiry and observation that audit trails are maintained for at least 5 years. Confirmed through inquiry and inspection that the log is reviewed and signed off by management. DFAS Saufley Field Confirmed through inquiry that audit trails are implemented for the application. Inspected the audit trails available and confirmed what information is being logged. Confirmed through inquiry and observation that audit trails are maintained for at least 5 years. Confirmed through inquiry and inspection that the log is reviewed and signed off by management.	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		12.1.3 DFAS Saufley Field 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.	DFAS Saufley Field Inspected the policy for protection of the audit trails and confirmed the policy limits access to audit trails. Confirmed through inquiry and observation that audit logs included activities that might modify, bypass, or negate safeguards controlled by the system and that Audit trails are protected against unauthorized access, modification, or deletion. Observed that only select/limited number of individuals such as the Information System Security officer (ISSO) and Information Assurance Manager have access to the audit trails.	No relevant exception noted.
12.4	Suspicious network access activity is investigated and appropriate action is taken. Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within DoD information systems.	12.4.2 DFAS Saufley Field DMI controls the configuration of computers and instant messaging program are not authorized. TSO PE monitors application usage through an automated software auditing application that runs regularly when users logon to their workstation. Instant messaging programs are identified as part of that auditing process.	DFAS Saufley Field Inquired with personnel to confirm that the use of instant messaging is against DoD policy and determined how they control instant messaging. Inspected firewall rules to confirm instant messaging is blocked.	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
13	**DCPS Change Management**			
13.1	DISA or DFAS initiated application, software, or hardware modifications are authorized, and the documentation is maintained.	13.1.1 DISA DECC Mechanicsburg Procedures addressing the testing of patches, upgrades, and new AIS applications are documented. All changes to information systems at DISA SMC-ME are brought before at least one of two Change Control Boards (CCBs). DISA headquarters has Executive software CCB which is responsible for reviewing all major system changes such as new versions, new software, and the removal of software. There is also a local CCB at DISA SMC-ME 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 the customer approval before proceeding. Also, the local CCB is responsible for maintaining the change control records. 13.1.2 DISA DECC Mechanicsburg The DISA Executive Software CCB consists of representatives of DISA management as well as all the DISA-SMCs. The DISA SMC-ME local	DISA DECC Mechanicsburg Obtained and inspected the change management policies and procedures for systems software to confirm that they exist and are current. Requested the full population of code/database modifications from the DCPS production code library which occurred during the audit period under review (7/01/06 through 6/30/07) and traced a sample of modifications to an approved System Change Request (SCR) or PTR. For each modification selected, obtained the change request document and confirmed that it was approved by key personnel prior to implementation. Confirmed that each modification was tested and the test results were approved prior to the modification being implemented. Confirmed the modification is documented by inspecting the SCR, System Test Plan (STP); detailed system specifications; and unit, system and acceptance testing results.	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		CCB consists of all department heads and the information assurance manager (IAM).		
		<u>13.1.3 DFAS Saufley Field</u> Testing of changes follows the approved process outlined in the DFAS TSO Business Process Handbook prior to implementation. A Testing Deficiency Report is issued for SCRs with negative test results and the TDR is routed to the appropriate individuals. If necessary, an amendment is issued and processes through same approval process as an SCR.	<u>DFAS Saufley Field</u> Using the same sample selected for control objective 13.1, confirmed that the DCPS application changes followed the appropriate test and migration process by inspecting the following for completeness, authorization and software quality requirements: • system test plan (STP); • detailed system specifications; and • unit, system and acceptance testing results. Inquired with DCPS security personnel as to their roles and responsibilities for the release of security-related changes included in DCPS Releases. Observed release notes for the major DCPS production releases that occurred during the audit period.	**<u>DFAS Saufley Field</u>** Two of the 45 sampled DFAS Saufley Field test scripts did not reference the SCR number. Testing results documentation was not maintained for 3 of the 45 sampled DFAS Saufley Field SCRs. No documentation exists which states which configuration items (CIs) are required to be tested prior to implementation. DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		13.1.4 DFAS Saufley Field Release management staff is responsible for ensuring that all programs are labeled and inventoried within the appropriate library.	DFAS Saufley Field Using the same sample selected for control objective 13.1, confirmed that the changes had been labeled, assigned an ID, and inventoried.	No relevant exception noted.
13.2	New and modified application, hardware, and operating system or utility software is tested and controlled according to specific criteria.	13.2.1 DFAS Saufley Field Release Management staff are responsible for distribution or implementation of new or revised software.	DFAS Saufley Field Using the same sample selected for control objective 13.1, confirmed that the change followed the appropriate distribution process by inspecting the release authorization report for completeness and authorization.	**DFAS Saufley Field** DFAS Saufley Field does not have a policy outlining what types of SCR configuration items (CI) are tested prior to implementation. DFAS management indicated the testing exception was caused by an administrative error and the exception was not significant enough to prevent the control activity from meeting its related control objective.
13.3	Emergency changes are promptly approved.	13.3.1 DFAS Saufley Field A configuration management plan is implemented for software modifications; contained in the DFAS TSO Business Process Handbook. All modifications must go through the system change request (SCR) process and receive proper	DFAS Saufley Field Using the same sample selected for control objective 13.1, confirmed through inspection that the DCPS emergency changes been authorized by the Program Manager and/or Software Director and traced each SCR or PTR identified above	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
		approvals prior to implementation, including emergency changes made during business hours. Emergency changes which 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.	to the Release Authorization Report to confirm it has been approved by the Software Director.	
13.4	Movement of programs and data among libraries is controlled.	13.4.1 DFAS Saufley Field The System Administrator manages access rights to the program libraries and databases through ACF2. The Database Administrator grants access to the appropriate development/production environments through IDMS. IDMS controls versioning in both the development and production environments.	DFAS Saufley Field Observed the DCPS Librarian to understand how the development and production libraries are controlled. Inspected the access control lists for the production and development libraries (directories) to confirm that only authorized personnel have access.	No relevant exception noted.
13.5	Use of public domain and personal software is restricted.	13.5.1 DFAS Saufley Field DFAS workstations and LANs do not allow any use of public domain and/or personal software. DCPS is on the mainframe; all utilities needed are on the mainframe (which is DISA-driven).	DFAS Saufley Field Inspected the DCPS SSAA to confirm that personal software is restricted. Inspected a list of approved software to confirm such a list exists. Confirmed by re-performance that the control to prevent the use of public domain software is operating effectively. .	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
13.6	Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.	13.6.1 DISA DECC Mechanicsburg All changes made at DISA SMC-ME are captured in the Change Management System (Change Management 2000). Information included in each change record is the requested time and date of implementation, the action to occur, and justification of the action. The change is then presented to the Change Control Board (CCB) where the change is assessed for IA and accreditation impact. The change is only implemented after approval from the CCB and testing is completed and reviewed 13.6.2 DFAS Saufley Field All changes made are captured in the Change Management Information System (CMIS). Information included in each change record is the requested time and date of implementation, the action to occur, and justification of the action. In addition, all changes are assessed by the IA Officers.	DISA DECC Mechanicsburg Using the same sample selected for control objective 13.1, obtained the CCB meeting minutes that included the discussion of the DCPS changes and confirmed whether management assessed the change for IA and accreditation impact. Established whether the changes were approved by the CCB and testing has been completed and approved prior to implementation into the production environment. DFAS Saufley Field Using the same sample selected for control objective 13.1, confirmed that the change record includes the requested time and date of implementation, the action to occur, and justification of the action.	No relevant exception noted.

No.	Control Objectives	Control Activities	Tests Performed	Results of Testing
14	**Data Retention**			
14.1	Data and program backup procedures have been implemented.	14.1.1 DFAS Saufley Field Data and program backup procedures have been established by DFAS Management DISA DECC Mechanicsburg Data and program backup procedures have been established by DFAS Management and are included in the DISA SMC ME Business Continuity Plan as prescribed in the SLA between DISA and DFAS.	DFAS Saufley Field Obtained the Business Continuity Plan to confirm that it specifies the data and program backup procedures that have been implemented related to DCPS. Inquired with key personnel that resources are dedicated to the periodic backing-up and restoration of data stored on network share drives. DISA DECC Mechanicsburg Obtained the Business Continuity Plan to confirm that it specifies the data and program backup procedures that have been implemented related to DCPS. Inquired with key personnel that resources are dedicated to the periodic backing-up and restoration of data stored on network share drives. Inquired how often backups are performed, shipped off site and maintained offsite in a fire rated container. Selected a sample of date's which occurred during the audit period and obtained the backup logs. Confirmed through inspection that the log is completed based upon the backup policies and procedures.	No relevant exception noted.

Section IV: Supplemental Information Provided by DFAS and DISA

IV. Supplemental Information Provided by DFAS and DISA

Introduction

DFAS and DISA have prepared this report section and it is included to provide information DFAS and DISA believes will be of interest to user organization. However, this information is not covered within the scope or control objectives established for the SAS 70 review. Specifically, this section includes a summary of procedures that DFAS and DISA have implemented to enable them to recover from a disaster affecting a Payroll Office, the TSOPE, or 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 an action plan to be implemented when a disaster or impending threat would render DCPS production support inoperable (for example, hurricane, damage to TSOPE facilities due to fire, etc.). This plan is evaluated and updated on an annual basis and is implemented locally at each of the established DCPS Payroll Offices. If an impending threat or event occurs, production support control for DCPS is transferred to an alternate-processing site. Currently, that site is DFAS Indianapolis, Indiana. The COOP includes the names of DCPS staff members who will serve as a pool of resources to be mobilized to execute the plan and a list of documentation and supplies that are necessary to support the mobilized team.

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

DECC 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 plan 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.

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

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

DFAS Indianapolis 592 Report Policies and Procedures

Policies and procedures for performing the 592 Payroll for Personal Services Payroll Certification and Summary Report reconciliation has not been developed and documented at the DFAS Indianapolis Payroll Office. DFAS Indianapolis has been using part of the DFAS Denver Payroll SOP and is developing a uniform DFAS Indianapolis SOP for performing the 592 Payroll for Personal Services Payroll Certification and Summary Report reconciliation as the office begins processing payroll for additional databases as the Denver Payroll office closes due to Base Realignment and Closure.

DCPS Password Configuration

The access control software for the environment on which DCPS resides, ACF2 supports complex passwords; however, complex passwords are not used. DISA and DFAS are in the process of transitioning the security configuration for the environment to allow for the use of the complex passwords.

Acronyms and Abbreviations

ACF2	Access Control Facility 2
ATO	Authority to Operate
BBG	Broadcast Board of Governors
BRAC	Base Realignment and Closure
CAC	Common Access Card
CBT	Computer Based Training
CCB	Configuration Control Board
COOP	Continuity of Operations Plan
CSR	Customer Service Representative
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
DoD	Department of Defense
DoE	Department of Energy
EOP	Executive Office of the President
EPA	Environmental Protection Agency
FSO	Field Security Operations
GCC	General Computer Controls
HHS	Health and Human Services
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alerts
IDMS	Integrated Database Management System
IS	Information Security
ISSO	Information System Security Officer
LANS	Local Area Networks
LPAR	Logical Partition
MAC	Mission Assurance Category
MOA	Memorandum of Agreement
NSA	National Security Agency
OIG	Office of the Inspector General
OLQ	Online Queries
PIIR	Personnel Interface Invalid Report
SAAR	Systems Access Authorization Request
SCR	System Change Request
SLA	Service Level Agreement
SMC	System Management Center

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

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 Directorate and Quantitative Methods Directorate, DoD OIG, also contributed to the report.

Paul J. Granetto
Patricia A. Marsh
Holly Williams
Frank C. Sonsini
Kenneth H. Stavenjord
Donna A. Roberts
Charles S. Dekle
Ernest G. Fine
Mary A. Hoover
Anissa M. Nash
Carl L. Adams
Debra J. DeJonge
Cassie C. Lin
Brian Royer
Kiana E. Silver
Alberto J. Calimano-Colon

Inspector General
Department of Defense