October 1, 2004

Information Technology Management

Report on Defense Civilian Pay System Controls Placed in Operation and Test of Operating Effectiveness for the Period March 1, 2004 through September 10, 2004
(D-2005-001)

Department of Defense
Office of the Inspector General

Constitution of the United States

A Regular Statement of Account of the Receipts and Expenditures of all public Money shall be published from time to time.

Article I, Section 9

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

October 1, 2004

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on the Defense Civilian Pay System (Report No. D-2005-001)

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. Addie M. Beima at (703) 604-9139 (DSN 664-9139) or Ms. Donna A. Roberts at (703) 604-9136 (DSN 664-9136). If management requests, we will provide a formal briefing on the results.

By direction of the Deputy Inspector General for Auditing

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

Table of Contents

Section I: Independent Service Auditors' Report

October 1, 2004

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on the Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness

We have examined the accompanying description of the general computer and application controls related to the Defense Civilian Pay System (DCPS) (Section II). DCPS is sponsored and used by the Defense Finance and Accounting Service (DFAS). The system is jointly maintained and technically supported by the Defense Information Systems Agency (DISA) and technical support elements of DFAS. 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 control 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 control contemplated in the design of the controls at DFAS and DISA; and (3) such controls had been placed in operation as of September 10, 2004.

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

The accompanying description includes only those application control objectives and related controls resident at the Charleston, SC, Pensacola, FL, and Denver, CO payroll offices and does not include application control objectives and related controls at the National Security Agency (NSA) payroll office. In addition, DCPS interfaces with over 50 DoD and external systems that either receive data from DCPS or transmit data to DCPS. Examples of these interfaces include the Defense Civilian Personnel Data System, Automated Time and Attendance and Production System, Automated Disbursing System, and Defense Joint Accounting System which perform personnel, timekeeping, disbursement, and payroll accounting functions. The accompanying description includes only the control objectives and related general and application controls resident at the Charleston, SC, Pensacola, FL, and Denver, CO payroll offices and related to the DCPS systems itself and does not include control objectives and related general and application controls resident at the NSA payroll office and related to the systems that interface with DCPS. Our examination did not extend to the controls resident at the NSA payroll office and related to the systems that interface with DCPS.

Our examination was conducted for the purpose of forming an opinion on the description of the DCPS general and application controls at DFAS and DISA (Section II). Information about business continuity plans and procedures at DFAS and DISA, as

provided by those organizations and included in Section IV, is presented to provide additional information to user organizations and is not a part of the description of controls at DFAS and DISA. The information in Section IV has not been subjected to the procedures applied in the examination of the aforementioned description of the controls at DFAS and DISA related to their business continuity plans and procedures and, accordingly, we express no opinion on the description of the business continuity plans and procedures provided by DFAS and DISA.

In our opinion, the accompanying description of the general computer and application controls at DFAS and DISA related to DCPS (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 September 10, 2004. 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 from March 1, 2004 to September 10, 2004. The specific control objectives; controls; and the nature, timing, extent, and results of the tests are listed 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.

As discussed in the accompanying description, a number of controls in place to ensure compliance with DoD information assurance policies, including DoDI 8500.2 and DITSCAP, appear to be suitably designed, but our tests of operating effectiveness indicated inconsistencies in adherence to these policies. Specifically, we noted the following:

- SDCA-1: Risk assessment activities performed at DECC-ME are not in full compliance with DoD 8510.1-M. Although a DITSCAP review had been completed, it had not been updated to reflect recent changes in the DITSCAP guidance. In addition, SRR reviews are regularly performed that should detect items not compliant with DISA standards.

- SDCA-1: Annual information assurance reviews as required by DoD 8510.1-M were not performed at TSOPE. However, DCPS is audited each year by various entities.

- SDCA-3: Extraneous communications services not covered by DISA STIGs are operating on all three logical partitions. While these extraneous services do not appear to pose significant risk to DCPS data, DoD information assurance policy states that for enclaves and AIS application, all DoD security configuration or implementation guides should be applied.

- SDCI-4: Several undocumented interfaces that are not covered by DISA STIGs were observed communicating with DCPS. While these interfaces do not appear to pose significant risk to DCPS data, DoD information assurance policy states that for enclaves and AIS application, all DoD security configuration or implementation guides should be applied.

As a result, the controls objectives SDCA-1, SDCA-3, and SDCI-4 may not have been achieved during the period from March 1, 2004 and September 10, 2004.

In our opinion, except for the deficiencies in operating effectiveness noted in the preceding paragraph, 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 from March 1, 2004 to September 10, 2004. However, the scope of our engagement did not include tests to determine whether control objectives not listed in Section III were achieved; accordingly, we express no opinion on the achievement of control objectives not included in Section III.

The relative effectiveness and significance of specific controls at DFAS and DISA and their effect on assessments of control risk at user organizations are dependent on their interaction with the internal control environment and other factors present at individual user organizations. We have performed no procedures to evaluate the effectiveness of internal controls placed in operation at individual user organizations.

The description of the controls at DFAS and DISA is as of September 10, 2004, and information about tests of their operating effectiveness covers the period from March 1, 2004 to September 10, 2004. 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 management of DCPS, its user organizations, and the independent auditors of such user organization.

By direction of the Deputy Inspector General for Auditing:

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, the Department of Defense (DoD) selected the Defense Civilian Pay System (DCPS) to serve as its standard payroll system for use by all DoD activities paying civilian employees, except Local Nationals and those funded by Non-appropriated Funds and Civilian Mariners. The DCPS program mission is to process payroll for the DoD civilian employees in accordance with existing regulatory, statutory, and financial information requirements relating to civilian pay entitlement and applicable policies and procedures. Beginning in 2003 and as part of the President's Management Agenda e-Payroll initiative, DFAS began processing payroll for Department of Energy (DOE) employees and was selected as one of four federal payroll providers to serve the entire executive branch of the Federal government. DFAS also processes payroll for the Executive Office of the President.

The DoD civilian pay program, including the payroll processing performed for DoD customers like DOE, 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 the various accounting, financial and personnel systems.

DCPS Support Functions

The Defense Finance and Accounting Service - Headquarters (DFAS-HQ) provides management control and coordination within DoD and has overall responsibility for interpretation and application of DCPS. The system is maintained and executed on the Defense Information Systems Agency (DISA) mainframe platforms at the Defense Enterprise Computing Center, Mechanicsburg (DECC-ME). The Technology Services Organization in Pensacola, Florida (TSOPE), which is part of DFAS, provides DCPS application support.

DCPS Systems Architecture

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

- *Mainframe hardware and software components* - used as a repository for the collection and accumulation of data, and to provide centralized, biweekly processing of civilian pay and its attendant functions (e.g., electronic funds transfer, generation of leave and earnings statements, etc.).

- *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 (e.g., reports, timesheets) at customer locations. These components are largely customer-owned and operated, and include personal computers, local area networks (LANs), a diverse assortment of printers, and the software that operates and connects them. A limited number of mid-tier (minicomputer) systems have been fielded by the Defense Finance and Accounting Service (DFAS) at selected DFAS sites to handle specialized printing requirements (e.g., paychecks). Other offloaded print services, such as bulk printing for DCPS payroll offices and printing of Leave and Earnings Statements (LES), are performed on PC/workstation hardware maintained by the Defense Automated Printing Service (DAPS) at DAPS sites located in various U.S. and overseas geographical regions.

The two tiers of the DCPS architecture are connected via DoD-maintained networks comprised of Internet Protocol (IP)-based (e.g., Non-Classified Internet Protocol Router Network (NIPRNET)) and Systems Network Architecture (SNA)-based (leased line) services. These networks connect DCPS to a wide variety of external, non-DCPS sites (mainframes, mid-tiers, and PCs) that supply or exchange data with DCPS on a regular basis, mainly through electronic file transfers. Examples of external interface sites include the Defense Civilian Personnel Data System, Federal Reserve, Thrift Savings Plan, Department of Treasury, and non-DoD users such as the Department of Energy and Executive Office of the President.

The main technical components of DCPS include the following attributes:

- DCPS is housed in a separate logical domain on an Amdahl 2045C mainframe computer located at DISA DECC-ME;
- The Amdahl operating system software is OS/390 release 2.8.0;
- DCPS is written in COBOL II language;
- First point of entry security protection mechanisms are provided by Access Control Facility 2 (ACF2) for OS/390;
- DECC-ME provides four web servers that service all applications that support DCPS. These 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 IDs and passwords; and
- Several third-party software packages are used for services associated with DCPS (e.g., process scheduling and monitoring).

Overview of Payroll Offices

Four payroll offices located in Charleston, SC; Denver, CO; Pensacola, FL; and at the National Security Agency (NSA), Fort Meade support the processing of all payroll transactions. The Customer Service Representatives (CSR) at each payroll office have access to the appropriate host system via dedicated leased lines and various DoD networks.

The payroll offices are structured in accordance with DFAS standard staffing policy and conduct business using standard operating and support procedures. They provide payroll service to customers located in various time zones and are responsible for the full range of pay processing functions and services that mainly include supporting and maintaining payroll transactions and resolution of issues and errors. The Charleston payroll office supports DoE payroll recipients and the Pensacola payroll office supports the Executive Office of the President payroll recipients.

Overview of System Interfaces

DCPS is a combination of on-line and batch programs that support the requirements of a bi-weekly, semimonthly, and in the case of the Executive Office of the President, monthly payroll. Transactions to update employee data, adjust leave balances, adjust payments for prior periods, and report time and attendance may be input daily to spread the online workload and to obtain labor data.

DCPS takes input from three main areas: CSRs located at the payroll offices; timekeepers; and personnel offices located throughout the DoD organization. As a result of this input and the output to external systems, DCPS receives or creates over 50 interface files that, among other functions, do the following:

- Update personnel information;
- Upload time and attendance data;
- Download information for checks to be printed;
- Report accounting information to the U.S. Treasury;
- Reconcile enrollment information with health care providers; and
- Download general accounting information to DoD agencies.

Automatic electronic file transfers directly to and from the host mainframe computer are used for most input and output file interfaces. Output files are automatically transferred to sites/activities using common file transfer protocols. CSRs must provide File Transfer Table data to TSOPE for table updates. For files not automatically transferred, it is the activity's responsibility to access the host computer to retrieve their output file(s) from the host. It is the responsibility of the activity creating an input interface file for DCPS to deliver it, by whatever means is available, to the payroll office or the processing center supporting the payroll office. A mutually agreeable schedule between the payroll activity and the submitting activity is established to help ensure timely receipt of data to support DCPS payroll processing.

Beginning in 2003, and as part of the President's Management Agenda e-Payroll initiative, DFAS began processing payroll for Department of Energy (DOE) employees and was selected as one of four federal payroll providers to service the entire executive branch of the Federal government. The migration of additional Executive Branch customers to DFAS is scheduled to be completed by September 2004. Through the consolidation process, efforts have been made to standardize payroll processing and delivery, which will drive additional interfaces and functionality.

B. Control Environment

DCPS Management Oversight

DFAS-HQ provides management control and coordination within the DoD and has overall responsibility for the DCPS system. DFAS-HQ is responsible for reviewing and maintaining the overall DCPS security policy. The TSOPE in Pensacola, FL, a unit of DFAS, provides DCPS software engineering, production support, and customer service. The TSOPE reports to the Civilian Pay Services business line at DFAS-HQ. The DCPS system is maintained and executed on DISA mainframe platforms at DECC-ME. DECC-ME is part of the Center for Computing Services within the Global Information Grid Combat Support Directorate, which is a Strategic Business Unit within DISA. DISA and DFAS are Defense Agencies that report to the Office of the Secretary of Defense. The support services provided by DISA to DCPS are documented in a signed service level agreement between DISA and DFAS. The service level agreement is reviewed and updated by both agencies on an annual basis. Both DFAS and DISA have documented policies and procedures for their respective functions.

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 systems security awareness training (2) securing civilians' and contractors' signature on an ADP Security Awareness disclosure, (3) identifying to the employee who their Terminal Area Security Officer (TASO) is and what the TASO's responsibilities are, and (4) notifying appropriate personnel to provide access or to immediately terminate employee and/or contractor access to DFAS automated information system (AIS) resources when an employee and/or contractor are processing-in or processing-out. The payroll offices and TSOPE facilities do not require any specific level of prior security clearance before a candidate can become an employee.

DISA DECC-ME

The Security Manager is responsible for the processing and vetting of new employees and contractors who are given access to DISA facilities in Mechanicsburg. All contractors and employees are required, at a minimum, to have a secret clearance and a positive National Agency Check (NAC). For employees, the Security Manager coordinates with the Personnel office and for contractors, the Security Manager coordinates with the contracting officer. The contracting officer is responsible for confirming that all contractors are assigned to a valid contract that has been approved to operate at DISA DECC-ME.

All new employees are required to sign DISA Form 312, which serves as a nondisclosure agreement for sensitive and classified information. When employees are terminated, they will sign the same Form 312 to confirm that they still understand the requirements put upon them. For new employees and contractors to

gain access to DISA systems, they are required to complete DISA Form 2875. The Security Manager is responsible for vetting these 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 itself. These reports are reviewed periodically and action is taken as necessary. All procedural problems and exceptions to normal or scheduled processing through hardware or software are logged, reported, and resolved in a timely manner, and action is taken as necessary.

In addition, several organizations within DoD perform monitoring associated with DCPS-related internal controls. These functions include:

DISA Office of the Inspector General and Field Security Office

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

In addition, DISA also has a Field Security Operations (FSO) unit that performs periodic reviews of DISA systems to determine whether those systems are in compliance with DISA's documented security standards. The DCPS system components that are maintained by DISA are subject to these FSO reviews. The FSO is independent of the DECC-ME management structure and does not maintain or configure DCPS systems.

DITSCAP Certification and Accreditation

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

DCPS is subject to the requirements of DITSCAP and must meet all of the DITSCAP certification and accreditation requirements throughout its life cycle. As part of the DCPS DITSCAP process, separate System Security Authorization Agreements (SSAAs) have been prepared for the DCPS application itself 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. These verification and validation procedures include, among other steps, vulnerability evaluations, security testing and evaluation, penetration testing, and risk management reviews.

Office of the Inspector General, Department of Defense

The Office of the Inspector General (OIG), Department of Defense was established by Congress to conduct and supervise audits and investigations related to the programs and operations of the DoD. The OIG reports directly to the Secretary of Defense and is independent of DFAS and DISA. DCPS, as well as the payroll processes it supports, is part of the OIG audit universe and is subject to financial, operational, and information technology audits, reviews, and special assessment projects.

D. Risk Assessment

The DITSCAP process, discussed in subsection C above, includes several activities that document and assess risks associated with DCPS. The DCPS application and enclave SSAAs, which are a product of the DITSCAP process, also document threats to DCPS and its supporting technical environment. The SSAAs also contain Residual Risk Assessments that document vulnerabilities noted during DCPS tests and analyses. The information contained in the SSAAs is updated on a periodic basis. Personnel from DFAS TSOPE and DISA DECC-ME participate in these risk assessment activities.

E. Information and Communication

Information Systems

DCPS is the information system used to process civilian payroll for DoD and its payroll customers, such as DOE. The processing of payroll involves over 50 different interfaces with DCPS. These interfaces are linked to other DoD financial systems as well as external systems. The majority of the interfaces are automated. All automated interfaces must conform to documented interface specifications developed by the TSOPE, who is responsible for executing and monitoring the automated interfaces.

Communication

The support relationship between DFAS and DISA DECC-ME is documented through a service level agreement that is reviewed and updated annually. The service level agreement outlines various DFAS and DISA DECC-ME points of contact and liaisons that should be used when DCPS issues arise. DISA DECC-

ME also assigns a customer relationship manager to work with DFAS TSOPE to resolve any DCPS processing problems or concerns.

Within DFAS, the TSOPE and payroll offices have a weekly meeting between the Directors and Managers of both organizations to discuss DCPS processing issues. There is also a Configuration Control Board, comprised of TSOPE and Payroll Office personnel, to review and approve functional and systemic changes to DCPS. The payroll offices also have a help desk function to identify and track user issues and problems with DCPS and communicate those issues and problems to the TSOPE for resolution.

F. Control Activities

The DCPS control objectives and related control activities are included in Section III of this report, "Information Provided by the Service Auditor," to eliminate the redundancy that would result from listing them in this section and repeating them in Section III. Although the control objectives and related controls are included in Section III, they are, nevertheless, an integral part of the description of controls.

G. User Organization Control Considerations

The control activities at DFAS and DISA 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 Information Systems Security Officer located at the payroll offices is notified of all terminated employees that are users of DCPS.
- their local Human Resource Office is notified of all terminated employees, so that such employees are removed from the Master Employee Record in a timely manner.
- all time entered by timekeepers is approved and authorized by appropriate user organization management.
- all Master Employee Records created represent valid employees.
- all changes to the Master Employee Record are approved by appropriate user organization personnel prior to payroll processing.
- segregation of duties exists between those at the user organization who enter time and those who enter or change Master Employee Records.
- if a pseudo Social Security Number (SSN) is created, the pseudo SSN has been authorized by appropriate user organization personnel and, if necessary, is accurately tied to a primary and valid SSN.
- user organization managers review the “Control of Hours” and other payroll-related reports for appropriateness and accuracy.

- all invalid interface feeds for time entry are reviewed and handled appropriately by appropriate user organization personnel and all invalid interface feeds for personnel records 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, Controls and Test of Operating Effectiveness

A. Scope Limitations

The control objectives documented in this section were specified by the Office of the Inspector General, Department of Defense. 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. The controls related to the source and destination systems associated with the DCPS interfaces are specifically excluded from this review. We did not perform procedures to evaluate the effectiveness of the input, processing, and output controls within these interface systems, although we did perform procedures to evaluate DCPS interface input and output controls. We did not perform any procedures to evaluate the integrity and accuracy of the data contained in DCPS.

B. Control Deficiencies

As a result of testing procedures described in the following matrix, operating effectiveness deficiencies were identified with certain control activities. In each instance where operating effectiveness deficiencies were identified, the audit team was able to identify and test additional controls that allowed the control objective to be achieved. These compensating controls and/or circumstances are documented with the description of the operating effectiveness deficiency in the following matrix.

In addition, the audit team identified certain compliance exceptions with DoD Information Assurance standards. These exceptions have been reported to DFAS and DISA management in a separate management report, but are not included herein as these exceptions do not adversely impact the achievement of the control objectives included in this Service Auditor's Report.

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

Accountability (AU)

Control Objective AU-1	Control Activity	Test of Controls	Test Results
Audit Record Content - Audit records include: • User ID; • Successful and unsuccessful attempts to access security files; • Date and time of the event. Type of event; • Success or failure of event. • Successful and unsuccessful logons; • Denial of access resulting from excessive number of logon attempts; • Blocking or blacklisting a user ID, terminal or access port, and the reason for the action; • Activities that might modify, bypass, or negate safeguards controlled by the system.	Audit records contain the following information: • User ID; • Successful and unsuccessful attempts to access security files; • Date and time of the event. Type of event; • Success or failure of event. • Successful and unsuccessful logons; • Denial of access resulting from excessive number of logon attempts; • Blocking or blacklisting a user ID, terminal or access port, and the reason for the action; • Activities that might modify, bypass, or negate safeguards controlled by the system.	Scanned identified audit logs for the presence of: • User ID; • Successful and unsuccessful attempts to access security files • Date and time of the event. Type of event; • Success or failure of event. • Successful and unsuccessful logons; • Denial of access resulting from excessive number of logon attempts; • Blocking or blacklisting a user ID, terminal or access port, and the reason for the action; • Activities that might modify, bypass, or negate safeguards controlled by the system.	No Relevant Exceptions Noted

Control Objective AU-2	Control Activity	Test of Controls	Test Results
Audit Trail, Monitoring, Analysis and Reporting - An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected.	DISA and DFAS policies specify the necessary procedures. The Service Level Agreement places the specific responsibility for the performance of the monitoring of various logs among both DISA and DFAS	Observed the operation of the system, including the most recent alerts. Interviewed the personnel monitoring the system to determine their knowledge of the procedures. Scanned manually maintained logs and records to determine that the appropriate audit functions are being performed.	No Relevant Exceptions Noted

Control Objective AU-3	Control Activity	Test of Controls	Test Results
Audit Trail Protection - The contents of audit trails are protected against unauthorized access, modification or deletion.	DISA and DFAS policies specify the necessary procedures. The Service Level Agreement places the specific responsibility for the performance of the monitoring of various logs among both DISA and DFAS	Scanned the DISA and DFAS security policies to confirm that they require adequate protection to the DCPS and operating system audit trails. Inspected the list of personnel with access to change the audit trail configuration. Observed the process for changing access to the audit trail information.	No Relevant Exceptions Noted

Master Files and Tables Accuracy (MFTA)

Control Objective MFTA – 1	Control Activity	Test of Controls	Test Results
Controls provide reasonable assurance that only valid and accurate changes are made to the payroll master files, payroll withholding tables and other critical system components; these changes are input and processed timely. .	Payroll master file and withholding data tables are periodically reviewed for accuracy and ongoing pertinence	Confirmed through corroborative inquiry with the appropriate payroll office management and functional users, that Payroll master file and withholding data tables are periodically reviewed for accuracy and ongoing pertinence.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies require that the master files and withholding tables be periodically reviewed.	No Relevant Exceptions Noted
		Scanned Online Line Query (OLQs) and reports to determine that master files and withholding tables are periodically reviewed.	No Relevant Exceptions Noted
1.2	Departmental managers periodically review listings of current employees within their departments and notify the personnel department of changes.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that Departmental managers periodically review listings of current employees within their departments and notify the personnel department of changes.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies require managers to periodically review employee listings and notify personnel departments of any changes.	No Relevant Exceptions Noted

		Scanned control of hours report noted they are sent to management for review of employee listings and notification to personnel departments of necessary changes.	No Relevant Exceptions Noted
1.3	Requests to change the payroll master file and withholding table data are logged; the log is reviewed to ensure that all requested changes are processed timely.	Confirmed through corroborative inquiry with the appropriate payroll office management and functional users that the changes to the payroll master file and withholding table data are logged and the log is reviewed to ensure that the requested changes are acceptable.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether it is required for changes to the payroll master file and withholding table data to be logged and the log is reviewed to ensure that the requested changes are acceptable.	No Relevant Exceptions Noted
		Scanned log of changes to payroll master file and withholding table to confirm change details are logged.	No Relevant Exceptions Noted
1.4	Changes to the payroll withholding tables and master files are compared to authorized source documents to ensure that they were input accurately.	Confirmed through corroborative inquiry appropriate TSO office management and functional users tax changes to the payroll withholding tables and master files are compared to source documents to ensure that the changes were tested and approved.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such procedures require that tax changes to the payroll withholding tables and master files are to be compared to source	No Relevant Exceptions Noted

		documents to ensure that they were tested and approved	
		Observed the process of tax changes to the payroll withholding tables and master files being compared to authorized source documents to ensure that they were tested and approved.	No Relevant Exceptions Noted
1.5	Requests to change the payroll master file data and withholding table are submitted on prenumbered forms; the numerical sequence of such forms is accounted for to ensure that the requested changes are processed timely. Access to source documents is controlled; Key source documents require signatures	Confirmed through corroborative inquiry with the appropriate payroll office management and functional users to confirm: • Requests to change the payroll master file data and withholding table are submitted on pre-numbered forms; • The numerical sequence of such forms is accounted for to ensure that the requested changes are processed timely; • Access to source documents is controlled; • Key source documents require signatures.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether the procedures exist to ensure: • Requests to change the payroll master file data and withholding table are submitted on pre-numbered forms; • The numerical sequence of such forms is accounted for to ensure that the requested changes are	No Relevant Exceptions Noted

		processed timely; • Access to source documents is controlled; • Key source documents require signatures.	
		Inspected haphazard sample of Remedy Tickets to confirm the requests: • Are prenumbered; • That the sequence is accounted for so that the forms are accounted for timely; • That access to the source documents is controlled; • That key source documents require signatures.	No Relevant Exceptions Noted
1.6	The source document is well-designed to aid the preparer and facilitate data entry. Transaction type and data field codes are preprinted on the source document.	Confirmed through corroborative inquiry appropriate payroll office management and functional users that the source document is appropriately designed to aid the preparer and facilitate data entry; and transaction type and data field codes are preprinted on the source document.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies require that the source documentation is required to be appropriately designed to aid the preparer and facilitate data entry, and that transaction type and data field codes are preprinted on the source document	No Relevant Exceptions Noted
		Observed the scanning and faxing of	No Relevant Exceptions Noted

		source documents to confirm it is appropriately designed to aid the preparer and facilitate data entry; and transaction type and data field codes are preprinted on the source document	
1.7	The ability to view, modify, or transfer information contained in the payroll master files is restricted to authorized personnel.	Confirmed through corroborative inquiry with the appropriate payroll office management and functional users that the ability to view, modify, or transfer information contained in the payroll master files is restricted to authorized personnel.	No Relevant Exceptions Noted
		Scanned policies and procedures determine whether the policies require the ability to view, modify, or transfer information contained in the payroll master files are restricted to authorized personnel.	No Relevant Exceptions Noted.
		Inspected haphazard sample of access forms to confirm the master file is restricted to authorized personnel	No relevant exceptions noted, however in performing our tests we noted that management had authorized a large number of personnel to use supervisor accounts. These numbers appear excessive given the access and responsibility these accounts maintain. In subsequent discussions with management, we noted these supervisor accounts are provided to authorized employees which DFAS feels need this level of access to perform their duties.

Control Objective MFTA-2	Control Activity	Test of Controls	Test Results
Controls provide reasonable assurance that payroll-related data, including gross pay, employer contributions, employee withholdings, taxes, leave, etc., is created or updated completely and accurately. Data validation and editing are performed to identify erroneous data. Erroneous data are captured, reported, investigated, and corrected.	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.	Confirmed through corroborative inquiry with the appropriate payroll office management and functional users that batch transactions without pre-assigned serial numbers are automatically assigned a unique sequence number, which is used by the computer to monitor that the transactions are processed.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether the policies require that the batch transactions without pre-assigned serial numbers are required to be automatically assigned a unique sequence number.	No Relevant Exceptions Noted
		Observed batch process monitoring and noted transactions without preassigned serial numbers are automatically assigned a unique sequence number.	No Relevant Exceptions Noted
2.2	Sequence checking is used to identify missing or duplicate batch transactions.	Confirmed through corroborative inquiry with the appropriate TSO office management and functional users that sequence checking is used to identify missing or duplicate batch transactions	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether the policies require that sequence checking is required to be used to identify missing or duplicate batch transactions.	No Relevant Exceptions Noted

		Observed the sequence checking to confirm it is used to identify missing or duplicate batch transactions.	No Relevant Exceptions Noted
2.3	Reports of missing or duplicate transactions are produced, and items are investigated and resolved in a timely manner.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that reports of missing or duplicate transactions are produced, and items are investigated and resolved timely.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies require that reports of missing or duplicate transactions are required to be produced, and items are be investigated and resolved timely.	No Relevant Exceptions Noted
		Scanned the Personnel Interface Invalid report of missing or duplicate transactions to confirm items are investigated and resolved timely.	Although testing confirmed that reports are reviewed and worked on daily basis, we noted that corrective actions are not sufficiently documented.
2.4	The source document is well-designed to aid the preparer and facilitate data entry. Transaction type and data field codes are preprinted on the source document.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that the source document is appropriately designed to aid the preparer and facilitate data entry; and transaction type and data field codes are preprinted on the source document.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies require source documentation to be appropriately designed to aid the preparer and facilitate data entry, and	No Relevant Exceptions Noted

		that transaction type and data field codes are preprinted on the source document.	
		Observed the scanning and faxing of source document to confirm that it is appropriately designed to aid the preparer and facilitate data entry; and transaction type and data field codes are preprinted on the source document.	No Relevant Exceptions Noted
2.5	Payroll master file data and withholding table data are edited and validated; identified errors are corrected promptly.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that the Payroll master file data and withholding table data are edited and validated; and identified errors are corrected promptly.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies require the Payroll master file data and withholding table data to be edited and validated; and identified errors are corrected promptly.	No Relevant Exceptions Noted
		Scanned Personnel Interface Invalid reports of missing or duplicate transactions to confirm items are investigated and resolved timely.	Although testing confirmed that reports are reviewed and worked on daily basis, we noted that corrective actions are not sufficiently documented.
2.6	Payroll withholding table data is periodically reviewed for compliance with statutory requirements.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that exceptions, based on parameters established by management, are reported for their review and approval.	No Relevant Exceptions Noted

		Scanned policies and procedures to determine whether such policies require exceptions, based on parameters established by management, to be reported for their review and approval.	No Relevant Exceptions Noted
		Scanned tax updates from BSI to confirm they are recalculated and subject to the change control process.	No Relevant Exceptions Noted
2.7	Exceptions, based on parameters established by management, are reported for their review and approval.	Confirmed through corroborative inquiry with the appropriate payroll office management and functional users that exceptions, based on parameters established by management, are reported for their review and approval.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies require exceptions, based on parameters established by management, to be reported for their review and approval.	No Relevant Exceptions Noted
		Scanned haphazard sample of exceptions on the L1OU and Employees Exceeding Limitations reports, based on parameters established by management, to confirm they are reported for their review and approval.	No Relevant Exceptions Noted

Accurate Payroll Processing (APP)

Control Objective APP-1	Control Activity	Test of Controls	Test Results
Controls provide reasonable assurance that payroll processing is accurate and recorded in the proper period. Payroll (including compensation and withholding) is accurately calculated and recorded. Controls provide reasonable assurance that disbursed payroll and related expense amounts are properly calculated. Controls provide reasonable assurance that prior period, current, and future period pay actions are based on effective dates	Compliance with the payroll disbursement processing schedule is monitored by management.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that compliance with the payroll disbursement processing schedule is monitored by management.	No Relevant Exceptions Noted
		Scanned policies and procedures and searched for a statement that compliance with the payroll disbursement processing schedule are monitored by management.	Policies and procedures are not detailed with specific guidance requiring that management monitor disbursing schedules.
.		Inspected pay processing schedules and observed payroll disbursement process and noted the monitoring of payroll disbursement processing schedule by management.	No relevant exceptions noted
1.2	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 a timely	Confirmed through corroborative inquiry with the appropriate payroll office management and functional users that the detailed payroll reconciliation shows pertinent data describing the payroll (including total disbursements,	No Relevant Exceptions Noted

	manner, to corresponding general ledger accounts within DCPS. All reconciling items are investigated and cleared on a timely basis, prior to disbursement	Retirement, TSP, Bonds, and other withholdings) and the related balances are reconciled, in a timely manner, to corresponding general ledger accounts within DCPS; and reconciling items are investigated and cleared prior to disbursement.	
		Scanned policies and procedures to determine whether such policies require the detailed payroll records show pertinent data describing the payroll (including total compensation, related income taxes, and other withholdings) and the related balances are reconciled, in a timely manner, to corresponding general ledger accounts or entries by persons who do not have unrestricted access to cash; and reconciling items to be investigated and cleared on a timely basis.	Policies and procedures are not detailed with specific guidance governing the reconciliation of and corrective action for reconciliation items. However, our testing confirms reconciling items are investigated and cleared on a timely basis, prior to disbursement
		Inspected a haphazard sample of "592" reconciliations for each database to confirm 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 a timely manner, to corresponding general ledger accounts within DCPS. Reconciling items are investigated and cleared on a timely basis, prior to disbursement	No Relevant Exceptions Noted

1.3	Record count and control totals established over source documents sent through the Imaging Center are used to help determine the completeness of data entry and processing.	Confirmed through corroborative inquiry with appropriate TSO office management and functional users, that record count and control totals established over source documents sent through the Imaging Center are used to help determine the completeness of data entry and processing.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies require record count and control totals established over source documents sent through the Imaging Center to be used to help determine the completeness of data entry and processing.	Policies and procedures are not detailed with specific guidance governing the control totals used at the Imaging Center. However, our testing confirms control totals exist at the Imaging Center.
		Observed the imaging of documents both manually scanned and faxed to confirm a unique sequence number is used to determine the completeness of processing.	No Relevant Exceptions Noted
1.4	For interfacing systems, record counts are accumulated and compared to footer control totals to help determine the completeness of interface processing.	Confirmed through corroborative inquiry with appropriate TSO office management and functional users, that for interfacing systems, record counts are accumulated and compared to footer control totals to help determine the completeness of interface processing.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies	No Relevant Exceptions Noted

		require interfacing systems, record counts to be accumulated and compared to footer control totals to help determine the completeness of interface processing.	
		Scanned interface files to confirm record counts match control totals in the footer to determine completeness of interface processing.	No Relevant Exceptions Noted
1.5	Payroll transactions at, before, or after the end of an accounting period are scrutinized and/or reconciled to ensure complete and consistent recording in the appropriate accounting period.	Confirmed through corroborative inquiry with the appropriate payroll office management and functional users that payroll transactions at, before, or after the end of an accounting period are scrutinized and/or reconciled to ensure complete and consistent recording in the appropriate accounting period.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies require payroll transactions at, before, or after the end of an accounting period to be scrutinized and/or reconciled to ensure complete and consistent recording in the appropriate accounting period.	Policies and procedures are not detailed with specific guidance requiring "592" reconciliations be performed in the appropriate accounting period. However, our testing confirms reconciliations are performed in the appropriate accounting period.
		Inspected a haphazard sample of "592" payroll reconciliations at, before, or after the end of an accounting period to confirm they are scrutinized and/or reconciled to ensure complete and consistent recording in the appropriate accounting period.	No Relevant Exceptions Noted

1.6	Standard programmed algorithms perform significant payroll calculations.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that tax table updates based on programmed algorithms are tested and approved prior to implementation.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies require tax table updates based on programmed algorithms to be tested and approved prior to implementation.	No Relevant Exceptions Noted
		Scanned tax table updates based on programmed algorithms to confirm they are tested and approved prior to implementation.	No Relevant Exceptions Noted
1.7	Programmed validation and edit checks identify erroneous data	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that programmed validation and edit checks identify erroneous data entered directly into DCPS.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies require programmed validation and edit checks to identify erroneous data entered directly into DCPS.	No Relevant Exceptions Noted
		Observed programmed validation and edit checks to confirm they identify erroneous data entered directly into	No Relevant Exceptions Noted

		DCPS.	
1.8	DCPS performs limit and reasonableness checks on employee earnings.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that programs perform limit and reasonableness checks on employee earnings.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies require programs to perform limit and reasonableness checks on employee earnings.	Policies and procedures are not detailed with specific guidance requiring that programs perform limit and reasonableness checks. However, our testing confirms limit and reasonableness checks exist.
		Scanned a limit and reasonableness report to confirm reasonableness checks are performed on employee earnings.	No Relevant Exceptions Noted
1.9	Summary payroll reports including total disbursements, Retirement, TSP, Bonds, and other withholdings) are reviewed and approved by management prior to disbursement.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that summary payroll reports including total disbursements, Retirement, TSP, Bonds, and other withholdings) are reviewed and approved by management prior to disbursement.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that summary payroll reports (including total disbursements, Retirement, TSP, Bonds, and other withholdings) are to be reviewed and approved by management prior to disbursement.	Policies and procedures are not detailed with specific guidance requiring that summary payroll reports (including total disbursements, Retirement, TSP, Bonds, and other withholdings) be reviewed by management prior to disbursement. However, our testing in Denver and

			Pensacola confirms reports are approved by management prior to disbursement.
		Inspected haphazard sample of "592" payroll reports (including total disbursements, Retirement, TSP, Bonds, and other withholdings) to confirm that they are reviewed and approved by management prior to disbursement.	In the Charleston payroll office, the persons who perform the reconciliation also perform the disbursement release creating the risk that disbursements could be sent to DFAS Cleveland for disbursement without proper approval. However, through corroborative inquiry of DFAS Charleston and DFAS Cleveland personnel, we confirmed that DFAS Cleveland has final responsibility for the disbursement of funds including net pay and requires a signed copy of the reconciliation before disbursement In addition, during our testing we noted that original signed copies of the reconciliation forms which are sent to DFAS Cleveland are not consistently maintained at payroll office.
1.10	Overtime hours worked and payments for such overtime are authorized by management for all salaried employees who are paid for overtime.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that overtime hours worked and payments for such overtime are authorized by management for salaried employees who are paid for overtime.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that overtime hours worked and payments for such overtime are	Policies and procedures are not detailed with specific guidance governing the approval of overtime

		authorized by management for salaried employees who are paid for overtime.	hours. However, we observed the performance of procedures that indicate reports are sent to departmental managers for review.
		Scanned control of hours report to confirm they are sent to management for salaried employees who are paid for overtime	No Relevant Exceptions Noted
1.11	Program code and criteria for tests of critical calculations are protected from unauthorized modifications.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that program code and criteria for tests of critical calculations are protected from unauthorized modifications.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that program code and criteria for tests of critical calculations are protected from unauthorized modifications.	No Relevant Exceptions Noted
		Observed program code and criteria for tests of critical calculations to confirm that the code and criteria is protected from unauthorized modifications.	No Relevant Exceptions Noted
1.12	Overriding or bypassing data validation and editing is restricted to supervisors and then only in a limited number of acceptable circumstances.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that overriding or bypassing data validation and editing is restricted to supervisors and then only in a limited number of acceptable circumstances.	No Relevant Exceptions Noted
		Scanned policies and procedures to identify guidance for overriding or	No Relevant Exceptions Noted

		bypassing data validation and editing, consistent with our discussions with staff.	
		Observed DCPS processing to confirm that overriding or bypassing data validation and editing is restricted to supervisors and then only in a limited number of acceptable circumstances.	No Relevant Exceptions Noted
1.13	Every override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that every override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness	No Relevant Exceptions Noted
		Scanned policies and procedures to identify guidance for overriding or bypassing data validation and editing, consistent with our discussions with staff.	No Relevant Exceptions Noted
		Observed input into DCPS and noted no overrides were needed.	No Relevant Exceptions Noted

Control Objective APP-2	**Control Activity**	**Test of Controls**	**Test Results**
Controls provide reasonable assurance that only valid, authorized employees are paid.	All payroll queries are followed up by persons independent of the payroll preparation and disbursement process	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that payroll queries are followed up by the Customer Service Department which is independent of the payroll preparation and disbursement process	No Relevant Exceptions Noted
		Scanned policies and procedures to	Policies and procedures are not

		confirm that payroll queries are to be followed up by persons independent of the payroll preparation and disbursement process	detailed with specific guidance governing the need for payroll queries to be followed up by persons independent of the payroll process However, our testing confirms that queries are reviewed by persons independent of the payroll process.
.		Inspected a haphazard sample of payroll queries to confirm they are followed up by persons independent of the payroll preparation and disbursement process.	No Relevant Exceptions Noted
2.2	Access to the payroll bank transfer tape is restricted to authorized personnel.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that access to the payroll bank transfer tape is restricted to authorized personnel.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that access to the payroll bank transfer tape is required to be restricted to authorized personnel.	No Relevant Exceptions Noted
		Inspected access listing to confirm access to the payroll bank transfer tape is restricted to authorized personnel.	No Relevant Exceptions Noted
2.3	Payroll master file and withholding data tables are periodically reviewed for accuracy and ongoing pertinence.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, Payroll master files are periodically reviewed for accuracy and ongoing pertinence.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that master files are required to be periodically reviewed.	Policies and procedures are not detailed with specific guidance governing the need for payroll master

			file data to be periodically reviewed for ongoing pertinence. However, our testing confirms payroll master file data are periodically reviewed for ongoing pertinence.
		Scanned Online Line Query (OLQs) and reports to determine that master files are periodically reviewed.	No Relevant Exceptions Noted
2.4	Departmental managers periodically review listings of current employees within their departments and notify the personnel department of changes.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, Departmental managers periodically review listings of current employees within their departments and notify the personnel department of changes.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that managers are required to periodically review employee listings and notify personnel departments of any changes.	No Relevant Exceptions Noted
		Scanned Personnel/Payroll Reconciliation and Control of Hours Reports to confirm they are sent to management for review of employee listings and notification to personnel department of changes.	No Relevant Exceptions Noted
2.5	A control log of output product errors is maintained, including the corrective actions taken.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, a control log of output product errors is maintained, including the corrective actions taken	No Relevant Exceptions Noted
		Scanned policies and procedures to identify the requirement for a control	No Relevant Exceptions Noted

		log of output product errors that are maintained, including the corrective actions taken.	
		Scanned control log of output product errors, known as the Personnel Interface Invalid report, to confirm it is maintained, including the corrective actions taken.	There is no preparer or supervisor sign-off on the control log. No details of corrective actions taken. However, reports are reviewed on a daily basis.
2.6	Payroll input data is edited and validated; identified errors are corrected promptly.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, payroll interface input data is edited and validated; identified errors are corrected promptly.	No Relevant Exceptions Noted
		Scanned policies and procedures to identify a requirement that the payroll interface input data is edited and validated; identified errors are corrected promptly.	No Relevant Exceptions Noted
		Scanned the Personnel Interface Invalid report of missing or duplicate transactions to confirm items are investigated and resolved timely.	Although testing confirmed that reports are reviewed and worked on daily basis, we noted that corrective actions are not sufficiently documented and that the preparer or supervisor sign-off is not consistently applied.
2.7	Time reported by employees is reconciled regularly between clock cards/timesheets and payroll reports.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that time reported by employees is reconciled regularly between clock cards/timesheets and payroll reports.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies	No Relevant Exceptions Noted

	require that time reported by employees is to be reconciled regularly between clock cards/timesheets and payroll reports.	
	Scanned report of time reported by employees to confirm that it is reconciled regularly between clock cards/timesheets and payroll reports.	No Relevant Exceptions Noted

Control Objective APP -3	**Control Activity**	**Test of Controls**	**Test Results**
Controls provide reasonable assurance of the reliability of DCPS data for financial reporting purposes. Data validation and editing are performed to identify erroneous data. Erroneous data are captured, reported, investigated, and corrected.	For batch application systems, batches are processed in sequence. Batch processing is observed real time to ensure jobs process appropriately.	Confirmed through corroborative inquiry with appropriate TSO office management and functional users that batch processing is performed in sequence. Scheduled jobs are monitored to ensure they are processing according to schedule.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine for batch application systems, batches are processed in sequence. Batch processing is observed real time to ensure jobs process appropriately.	No Relevant Exceptions Noted
.		Observed batch process monitoring and noted that batch processing is monitored real time and batches are processed in sequence.	No Relevant Exceptions Noted
3.2	Record counts and control totals are established over the suspense file.	Confirmed through corroborative inquiry with appropriate TSO office management and functional users, that record counts and control totals are established over the suspense file.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that record counts and control totals are established over the	No Relevant Exceptions Noted

		suspense file.	
		Inspected record counts and control totals to confirm they are established over the suspense file.	No Relevant Exceptions Noted
3.3	A control group is responsible for controlling and monitoring rejected transactions	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that a control group is responsible for controlling and monitoring rejected transactions	No Relevant Exceptions Noted
		Scanned policies and procedures to determine that a control group is responsible for controlling and monitoring rejected transactions	No Relevant Exceptions Noted
		Scanned the Personnel Interface Invalid report to confirm the report is used for controlling and monitoring rejected transactions.	No Relevant Exceptions Noted
3.4	Authorization profiles effectively protect the suspense file from unauthorized access and modification.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that authorization profiles effectively protect the suspense file from unauthorized access and modification.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that general controls effectively protect the suspense file from unauthorized access and modification	No Relevant Exceptions Noted
		Observed authorization profiles to confirm that they effectively protect the suspense file from unauthorized access and modification	No Relevant Exceptions Noted
3.5	Rejected data are automatically	Confirmed through corroborative	No Relevant Exceptions Noted

	written on an automated error suspense file and held until corrected, 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.	inquiry with appropriate payroll office management and functional users that rejected data are automatically written on an automated error suspense file and held until corrected, 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.	
		Scanned policies and procedures to confirm that rejected data are required to be automatically written on an automated error suspense file and held until corrected, 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.	No Relevant Exceptions Noted
		Scanned the Personnel Interface Invalid report of rejected data to confirm that the rejected data are automatically written on an automated error suspense file and held until corrected, 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.	No Relevant Exceptions Noted

3.6	The suspense file is purged of transactions as they are corrected.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that the suspense file is purged of transactions as they are corrected.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine that the suspense file is purged of transactions as they are corrected.	No Relevant Exceptions Noted
		Scanned the Personnel Interface Invalid report of missing or duplicate transactions and through corroborative inquiry confirmed the suspense file is purged of transactions as they are corrected.	Although testing confirmed that reports are reviewed and worked on daily basis, we noted that corrective actions are not sufficiently documented and that the preparer or supervisor sign-off is not consistently applied.
3.7	The suspense file is used to produce, on a regular basis and for management review, an analysis of the level and type of transaction errors and the age of uncorrected transactions.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that the suspense file is used to produce, on a regular basis and for management review, an analysis of the level and type of transaction errors and the age of uncorrected transactions.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that the suspense file is required to be used to produce, on a regular basis and for management review, an analysis of the level and type of transaction errors and the age of uncorrected transactions.	No Relevant Exceptions Noted
		Scanned the Personnel Invalid Report to confirm the report is used to produce, on a regular basis and for	No Relevant Exceptions Noted

		management review, an analysis of the level and type of transaction errors and the age of uncorrected transactions.	
3.8	Error reports or error files accessible by computer terminal show rejected transactions with error messages that have clearly understandable corrective actions for each type of error.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that error reports or error files accessible by computer terminal show rejected transactions with error messages that have clearly understandable corrective actions for each type of error.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that error reports or error files accessible by computer terminal are required to show rejected transactions with error messages that have clearly understandable corrective actions for each type of error.	No Relevant Exceptions Noted
		Scanned error reports or error files accessible by computer terminal to confirm they show rejected transactions with error messages that have clearly understandable corrective actions for each type of error.	No Relevant Exceptions Noted
3.09	All corrections are reviewed and approved by supervisors before the corrections are reentered.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that corrections are reviewed and approved by supervisors before the corrections are reentered.	There is no supervisor signature on error report to signify review of technician's corrective actions. However, reports are reviewed on a daily basis.
		Scanned policies and procedures to	Policies and procedures are not

	confirm that corrections are to be reviewed and approved by supervisors before the corrections are reentered.	detailed with specific guidance requiring corrections to be reviewed and approved by supervisors. However, we observed the performance of procedures that indicate corrections are reviewed and approved by Supervisors.
	Scanned error report, Personnel Interface Invalid, to confirm the report is reviewed and approved by supervisors before the corrections are reentered.	Although testing confirmed that reports are reviewed and worked on daily basis, we noted that corrective actions are not sufficiently documented and that the preparer or supervisor sign-off is not consistently applied.

Control Objective APP-4	**Control Activity**	**Test of Controls**	**Test Results**
Controls provide reasonable assurance 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. Controls provide reasonable assurance that current- or prior-period adjustments to employee's pay, i.e. employee debt, tax deduction or deductions not taken, are reported, reconciled and approved.	Payroll transactions at, before, or after the end of an accounting period are scrutinized and/or reconciled to ensure complete and consistent recording in the appropriate accounting period	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that payroll transactions at the end of a payroll cycle are reconciled to ensure complete and consistent recording in the appropriate accounting period.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that payroll transactions at, before, or after the end of an accounting period are required to be scrutinized and/or reconciled to ensure complete and consistent recording in the appropriate	Policies and procedures are not detailed with specific guidance requiring “592” reconciliations be performed in the appropriate accounting period. However, , our testing confirms we observed the performance of procedures that

		accounting period.	indicate the reconciliations are performed in the appropriate accounting period.
		Inspected haphazard sample of "592" payroll reconciliations at the end of a payroll cycle to confirm they are reconciled to ensure complete and consistent recording in the appropriate accounting period.	No Relevant Exceptions Noted
4.2	Payroll withholding table data is periodically reviewed for compliance with statutory requirements.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, payroll withholding table data is periodically reviewed for compliance with statutory requirements.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that payroll withholding table data is required to be periodically reviewed for compliance with statutory requirements	No Relevant Exceptions Noted
		Inspected a haphazard sample of payroll withholding table data updates to confirm they are periodically updated for compliance with statutory requirements.	No Relevant Exceptions Noted
4.3	The data processing control group, or some alternative •has a schedule by application that shows when outputs are to be completed, when they need to be distributed, who the recipients are, and the copies needed; •reviews output products for general acceptability; and	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, the data processing control group, or some alternative • Has a schedule by application that shows when outputs are completed, when they need to be	No Relevant Exceptions Noted

	•reconciles control information to determine completeness of processing.	distributed, who the recipients are, and the copies needed; • Review output products for general acceptability; • Reconciles control information to determine completeness of processing.	
		Scanned policies and procedures to confirm that the data processing control group, or some alternative, • Has 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; • Reviews output products for general acceptability; • Reconciles control information to determine completeness of processing.	Policies and procedures are not detailed with specific guidance that a data processing control group reviews output products and has a schedule of completed outputs. However, our testing confirms a data processing control group reviews product outputs.
		Scanned 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; • Reviews output products for general acceptability; • Reconcile control information to determine completeness of processing	No Relevant Exceptions Noted
4.4	Users review output reports for data accuracy, validity, and completeness. The reports include	Confirmed through corroborative inquiry with appropriate payroll office management and functional	No Relevant Exceptions Noted

	•error reports• •master record change reports, •exception reports	users, users review output reports for data accuracy, validity, and completeness. The reports include • Error reports; • Master record change reports; • Exception reports.	
		Scanned policies and procedures to determine whether such policies require users to review output reports for data accuracy, validity, and completeness. The reports include • Error reports; • Master record change reports; • Exception reports.	Policies and procedures were not detailed with specific guidance that output errors included error and transaction reports, and master record change reports. However, our testing confirms that output errors include error and transaction reports.
		Scanned the Personnel Interface Invalid report users review for output to confirm the reports are reviewed data accuracy, validity, and completeness. The reports include • Error reports; • Master record change reports; • Exception reports.	No Relevant Exceptions Noted
4.5	Programmed validation and edit checks identify erroneous data.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that programmed validation and edit checks identify erroneous data entered directly into DCPS.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that programmed validation and edit checks identify erroneous data are required to be entered directly into DCPS	No Relevant Exceptions Noted
		Observed programmed validation and edit checks to confirm that they	No Relevant Exceptions Noted

		identify erroneous data entered directly into DCPS.	
4.6	The detailed payroll reconciliation shows pertinent data describing the payroll (including total disbursements, Retirement, Thrift Savings Plan (TSP), Bonds, and other withholdings) and the related balances are reconciled, in a timely manner, to corresponding general ledger accounts within DCPS. All reconciling items are investigated and cleared on a timely basis, prior to disbursement	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that 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 a timely manner, to corresponding general ledger accounts within DCPS. Reconciling items are investigated and cleared on a timely basis, prior to disbursement.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that the detailed payroll records show pertinent data describing the payroll (including total compensation, related income taxes, and other withholdings) and the related balances are to be reconciled, in a timely manner, to corresponding general ledger accounts or entries by persons who do not have unrestricted access to cash; and reconciling items are investigated and cleared on a timely basis.	Policies and procedures are not detailed with specific guidance requiring "592" reconciliations be performed and how to handle reconciling items. However our testing confirms that reconciling items are handled appropriately.
.		Inspected haphazard sample of "592" reconciliation for each database and noted detailed payroll records show pertinent data describing the payroll (including total compensation,	No Relevant Exceptions Noted

	related income taxes, and other withholdings) and the related balances are reconciled, in a timely manner, to corresponding general ledger accounts or entries by persons who do not have unrestricted access to cash. Reconciling items are investigated and cleared on a timely basis.	

Control Objective APP-5	Control Activity	Test of Controls	Test Results
Controls provide reasonable assurance that data transmissions between DCPS and user organizations are authorized, complete, accurate and secure. All application users are appropriately identified and authenticated. Access to the application and output is restricted to authorized users for authorized purposes.	All transactions are logged as entered, along with the terminal ID and the ID of the person entering the data.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that transactions are logged as entered, along with the terminal ID and the ID of the person entering the data.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that transactions are to be logged as entered, along with the terminal ID and the ID of the person entering the data.	No Relevant Exceptions Noted
		Observed the operation of the system, including the most recent alerts. Interviewed the personnel monitoring the system to determine their knowledge of the procedures. Scanned manually maintained logs and records to determine that the appropriate audit functions are being performed.	No Relevant Exceptions Noted
5.2	Significant fields are rekeyed or error messages are available to verify the accuracy of data entry.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that significant fields are rekeyed or error messages are available to verify the accuracy of data entry.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that they require significant fields are rekeyed or error messages	No Relevant Exceptions Noted

		are available to verify the accuracy of data entry.	
		Observed significant fields and noted error messages are available to verify the accuracy of data entry.	No Relevant Exceptions Noted
5.3	Effective use is made of automated entry or error detection mechanisms to reduce the potential for data entry errors.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users effective use is made of automated entry or error detection mechanisms to reduce the potential for data entry errors.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that effective use is made of automated entry or error detection mechanisms are required to reduce the potential for data entry errors.	No Relevant Exceptions Noted
		Observed user entering data to confirm error reporting exists.	No Relevant Exceptions Noted
5.4	On-line access logs are maintained by the system, and the logs are reviewed regularly for unauthorized access attempts.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users that on-line access logs are maintained by the system, and the logs are reviewed regularly for unauthorized access attempts.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that on-line access logs are required to be maintained by the system, and the logs are reviewed regularly for unauthorized access attempts.	No Relevant Exceptions Noted
		Scanned haphazard sample of e-mail for unauthorized access attempts to confirm that they are maintained by	No Relevant Exceptions Noted

		the SMO, and the logs are reviewed regularly for unauthorized access attempts.	
5.5	Each operator is required to have a completed and approved authorization form before being granted access to the system.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that each operator is required to have an authorization form before being granted access to the system.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that each operator is required to have an authorization form before being granted access to the system.	No Relevant Exceptions Noted
		Inspected a haphazard sample of user authorization forms to confirm that each operator is required to have an authorization form before being granted access to the system.	Out of twenty-three user authorization forms selected for testing in Charleston, noted one where the user's form could not be located and ten where access granted could not match access approved. Out of nineteen user authorization forms selected for testing Pensacola, noted one account where an authorization form did not exist, and two where access granted did not match access provided. For those whose access represented supervisor or equivalent access, management concurred with the level of access provided.
5.6	Supervisors sign on to each terminal device, or authorize terminal usage from a program file server, before an	Confirmed through corroborative inquiry with appropriate payroll office management and functional	No Relevant Exceptions Noted

	operator can sign on to begin work for the day.	users, that Supervisors sign on to each terminal device, or authorize terminal usage from a program file server, before an operator can sign on to begin work for the day.	
		Scanned policies and procedures to confirm that Supervisors are required to sign on to each terminal device, or authorize terminal usage from a program file server, before an operator can sign on to begin work for the day.	No Relevant Exceptions Noted
		Observed sign on process to confirm that Supervisors sign on to each terminal device, or authorize terminal usage from a program file server, before an operator can sign on to begin work for the day.	No Relevant Exceptions Noted
5.7	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.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that 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.	No Relevant Exceptions Noted
		Scanned policies and procedures confirm that data entry terminals are to be connected to the system only during specified periods of the day, which corresponds with the business hours of the data entry personnel.	No Relevant Exceptions Noted
		Observed after-hours processes to confirm terminals are not authorized to be connected after business hours.	No Relevant Exceptions Noted

5.8	Each terminal automatically disconnects from the system when not used after a specified period of time.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that each terminal automatically disconnects from the system when not used after a specified period of time.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that each terminal is required to automatically disconnect from the system when not used after a specified period of time.	No Relevant Exceptions Noted
		Observed system inactivity to confirm that each terminal automatically disconnects from the system when not used after a specified period of time.	No Relevant Exceptions Noted
5.9	When terminals are not in use, terminal rooms are locked, or the terminals are capable of being secured.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that when terminals are not in use, terminal rooms are locked, or the terminals are capable of being secured.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine that when terminals are not in use, terminal rooms are required to be locked, or the terminals are capable of being secured.	No Relevant Exceptions Noted
		Observed the facilities confirm that when terminals are not in use, terminal rooms are locked, or the terminals are capable of being secured.	No Relevant Exceptions Noted
5.10	Data entry terminals are located in	Observed that data entry terminals	No Relevant Exceptions Noted

	physically secure rooms.	are located in physically secure rooms	
		Scanned policies and procedures to confirm that data entry terminals are required to be located in physically secure rooms.	No Relevant Exceptions Noted
		Observed the facilities to confirm that data entry terminals are located in physically secure rooms.	No Relevant Exceptions Noted
5.11	Remote terminal connections are secured and are connected via government computers	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that remote terminal connections are secured and are connected via government computers	Users have the ability to logon from home via remote connection from their non-government issued personal computers. However, in order to gain access to DCPS all users must also authenticate with a valid DCPS username and password regardless of whether they connect remotely or from their office.
		Scanned policies and procedures to confirm that remote terminal connections are required to be secured and are connected via government computers	No Relevant Exceptions Noted
		Observed remote terminal connections to confirm they are secured and are connected via government computers	Users have the ability to logon from home via remote connection from their non-government issued personal computers. However, in order to gain access to DCPS all users must also authenticate with a valid DCPS username and password regardless of whether they connect remotely or from their office.
5.12	Authorization profiles over terminals limit what transactions can be entered from a given terminal.	Confirmed through corroborative inquiry with appropriate payroll office management and functional	No Relevant Exceptions Noted

		users, that authorization profiles over terminals limit what transactions can be entered from a given terminal.	
		Scanned policies and procedures to confirm that authorization profiles over terminals are required to limit what transactions can be entered from a given terminal.	Policies and procedures are not detailed with specific guidance restricting the number of accounts with Supervisor access or Master Employee Record (MER) update and Time and Attendance (T/A).access. However, our inquires confirm these accounts are given to authorized employees which DFAS feels need this level of access to perform their duties.
		Inspected haphazard sample of user authorization forms to confirm that authorization profiles limit what transactions can be entered from a given terminal.	No relevant exceptions noted, however in performing our tests we noted that management had authorized a large number of personnel to use personnel accounts. These numbers appear excessive given the access and responsibility these accounts maintain. In subsequent discussions with management, we noted these supervisor. accounts are provided to authorized employees which DFAS feels need this level of access to perform their duties.
5.13	Authorization profiles over users limit what transactions data entry personnel can enter.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that authorization profiles over users limit what transactions data entry personnel can enter.	No Relevant Exceptions Noted

		Scanned policies and procedures to confirm that user authorization profiles are required to limit what transactions data entry personnel can enter.	No Relevant Exceptions Noted
		Inspected haphazard sample of user authorization profiles to confirm they limit what transactions can be entered from a given terminal.	No Relevant Exceptions Noted
5.14	Preformatted computer terminal screens are utilized and allow prompting for data to be entered, and editing of data as it is entered.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that preformatted computer terminal screens are utilized and allows prompting for data to be entered, and editing of data as it is entered.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that user authorization profiles are required to limit what transactions data entry personnel can enter.	No Relevant Exceptions Noted
		Observed haphazard sample of screen shot of preformatted computer terminal screens to confirm they are utilized and allow prompting for data to be entered, and editing of data as it is entered.	No Relevant Exceptions Noted

Control Objective APP -6	**Control Activity**	**Test of Controls**	**Test Results**
Controls are reasonable to ensure that transactions from interfacing systems are subjected to the payroll system edits, validations and error-correction procedures.	Computer generated record counts and control totals are established over and entered with batch transaction data, and reconciled to determine the completeness of data entry.	Confirmed through corroborative inquiry with appropriate TSO office management and functional users, that record counts and control totals are established over and entered with	No Relevant Exceptions Noted

		batch transaction data, and reconciled to determine the completeness of data entry.	
		Scanned policies and procedures to determine whether such policies require record counts and control totals to be established over and entered with batch transaction data, and reconciled to determine the completeness of data entry.	No Relevant Exceptions Noted
.		Scanned record counts and control totals to confirm they are established over and entered with batch transaction data, and reconciled to determine the completeness of data entry.	No Relevant Exceptions Noted
6.2	Trailer labels or control records containing record counts and control totals are generated for all computer files and tested by application programs to determine that all records have been processed.	Confirmed through corroborative inquiry with appropriate TSO office management and functional users, that trailer labels or control records containing record counts and control totals are generated for computer files and tested by application programs to determine that records have been processed successfully.	No Relevant Exceptions Noted
		Scanned policies and procedures and to confirm that trailer labels or control records containing record counts and control totals are required to be generated for computer files and tested by application programs to determine that records have been processed successfully.	No Relevant Exceptions Noted
		Scanned trailer labels or control records containing record counts and	No Relevant Exceptions Noted

		control totals to confirm they are generated for computer files and tested by application programs to determine that records have been processed successfully.	
6.3	A data processing control group receives and reviews control total reports, and determines the completeness of processing.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that a data processing control group receives and reviews control total reports, and determines the completeness of processing.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that a data processing control group is required to receive and review control total reports, and determine the completeness of processing.	No Relevant Exceptions Noted
		Scanned the Personnel Interface Invalid report to confirm a data processing control group receives and reviews control total reports, and determines the completeness of processing.	Although testing confirmed that reports are reviewed and worked on daily basis, we noted that corrective actions are not sufficiently documented and that the preparer or supervisor sign-off is not consistently applied.
6.4	Reconciliations are performed to determine the completeness of transactions processed, master files updated, and outputs generated.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that reconciliations are performed to determine the completeness of transactions processed, master files updated, and outputs generated.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that reconciliations are to be	Policies and procedures are not detailed with specific guidance

		performed to determine the completeness of transactions processed, master files updated, and outputs generated.	requiring "592" reconciliations be performed and how to handle reconciling items. However, our testing confirms that reconciling items are completed appropriately
		Inspected haphazard sample of "592" reconciliations to confirm that they are performed to determine the completeness of transactions processed, master files updated, and outputs generated.	No Relevant Exceptions Noted
6.5	Computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing	Confirmed through corroborative inquiry with appropriate TSO office management and functional users, that computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that computer-generated control totals (run-to-run totals) are required to be automatically reconciled between jobs to check for completeness of processing.	No Relevant Exceptions Noted
		Scanned record counts and control totals to confirm they are established over and entered with transaction data, and reconciled to determine the completeness of data entry.	No Relevant Exceptions Noted
6.6	System interfaces require that the sending system's output control counts equal the receiving system's determined input counts.	Confirmed through corroborative inquiry with appropriate TSO office management and functional users, that system interfaces require that the sending system's output control	No Relevant Exceptions Noted

		counts equal the receiving systems determined input counts.	
		Scanned policies and procedures to confirm that system interfaces require that the sending system's output control counts equal the receiving system's determined input counts.	No Relevant Exceptions Noted
		Scanned record counts and control totals to confirm interfaces require that the sending system's output control counts equal the receiving system's determined input counts.	No Relevant Exceptions Noted
6.7	Program code for data validation and editing, and associated tables or files are protected from unauthorized modifications.	Confirmed through corroborative inquiry with appropriate TSO office management and functional users, that program code for data validation and editing and associated tables or files are protected from unauthorized modifications.	No Relevant Exceptions Noted
		Scanned policies and procedures to determine whether such policies require program code for data validation and editing and associated tables or files to be protected from unauthorized modifications.	No Relevant Exceptions Noted
		Scanned access logs to confirm only users authorized have access to the system software.	No Relevant Exceptions Noted

Control Objective APP-7	**Control Activity**	**Test of Controls**	**Test Results**
Controls are reasonable to ensure that transactions from interfacing systems are subjected to the payroll system edits, validations and error-correction	The data processing control group, or some alternative •has a schedule by application that shows when outputs are to be	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, the data processing control	No Relevant Exceptions Noted

procedures. Data validation and editing are performed to identify erroneous data. Erroneous data are captured, reported, investigated, and corrected.	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.	group, or some alternative • Has a schedule by application that shows when outputs are to 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.	
		Scanned policies and procedures to confirm that the data processing control group, or some alternative • Have a schedule by application that shows when outputs are 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.	Policies and procedures are not detailed with specific guidance requiring that management monitor disbursing schedules. However, we observed the performance of procedures that indicate management is monitoring disbursing schedules.
		Scanned haphazard sample of schedules used by the data processing group, and noted • Has 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; • Reviews output products for general acceptability; and • Reconciles control information	No Relevant Exceptions Noted

		to determine completeness of processing.	
7.2	Printed reports contain a title page with report name, time and date of production, the processing period covered; and have an "end-of-report" message.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, printed reports contain a title page with report name, time and date of production, the processing period covered; and have an "end-of-report" message.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm printed reports are required to contain a title page with report name, time and date of production, the processing period covered; and have an "end-of-report" message	No Relevant Exceptions Noted
		Scanned haphazard sample of printed reports to confirm they contain a title page with report name, time and date of production, the processing period covered;	No Relevant Exceptions Noted
7.3	Each output produced is logged, manually if not automatically, including the recipient(s) who receive the output. Each transmission of output to a user's terminal device is also logged.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, each output produced is logged, manually if not automatically, including the recipient(s) who receive the output. Each transmission of output to a user's terminal device is also logged	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that each output produced is to be logged, manually if not automatically, including the recipient(s) who receive the output.	Policies and procedures are not detailed with specific guidance requiring that each output be logged including the user's terminal and the recipient However, we observed the

		Each transmission of output to a user's terminal device is also logged.	performance of procedures that indicate these reports are being reviewed regularly.
		Observed MECSAR to confirm reports are logged, manually if not automatically, including the recipient(s) who receive the output. Each transmission of output to a user's terminal device is also logged	No Relevant Exceptions Noted
7.4	A control log of output product errors is maintained, including the corrective actions taken.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, a control log of output product errors is maintained, including the corrective actions taken	No Relevant Exceptions Noted
		Scanned policies and procedures to identify the requirement for a control log of output product errors are to be maintained, including the corrective actions taken.	No Relevant Exceptions Noted
		Scanned the Personnel Interface Invalid report of missing or duplicate transactions to confirm it is maintained, including the corrective actions taken.	Although testing confirmed that reports are reviewed and worked on daily basis, we noted that corrective actions are not sufficiently documented.
7.5	Output from reruns is subjected to the same quality review as the original output.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, output from reruns are subjected to the same quality review as the original output.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that output from reruns are subjected to the same quality review as the original output.	No Relevant Exceptions Noted

		Scanned Personnel Interface Invalid report to confirm it is subjected to the same quality review as the original output.	No Relevant Exceptions Noted
7.6	Users review output reports for data accuracy, validity, and completeness. The reports include: •error reports •master record change reports, and, •exception reports	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, users review output reports for data accuracy, validity, and completeness. The reports include: • Error reports; • Master record change reports; • Exception reports.	No Relevant Exceptions Noted
		Scanned policies and procedures and noted users review output reports for data accuracy, validity, and completeness. The reports include: • Error reports • Master record change reports; • Exception reports.	Policies and procedures are not detailed with specific guidance requiring that users review output reports for accuracy, validity, and completeness. However, we observed the performance of procedures that indicate reports are reviewed for validity and completeness.
		Scanned Personnel Interface Invalid report users review for accuracy, validity, and completeness. The reports include: • Error reports; • Master record change reports; • Exception reports.	No Relevant Exceptions Noted
7.7	For on-line or real-time systems, record count and control totals are accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness or data entry and processing.	Confirmed through corroborative inquiry with appropriate TSO office management and functional users, for on-line or real-time systems, record count and control totals are accumulated progressively for a specific time period (daily or more	No Relevant Exceptions Noted

		frequently) and are used to help determine the completeness or data entry and processing.	
		Scanned policies and procedures to confirm that on-line or real-time systems, record count and control totals are required to be accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness or data entry and processing.	No Relevant Exceptions Noted
		Scanned record counts and control total interface files to confirm they are accumulated progressively for a specific time period (daily or more frequently) and are used to help determine the completeness or data entry and processing.	No Relevant Exceptions Noted

Control Objective APP-8	**Control Activity**	**Test of Controls**	**Test Results**
Controls provide reasonable assurance that personnel payroll records and other sensitive information is maintained and disposed of in accordance with Government-wide and agency specific guidelines.	All documents and storage media are stored in physically and environmentally secure containers.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, documents and storage media are stored in physically and environmentally secure containers.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that documents and storage media are stored in physically and environmentally secure containers.	No Relevant Exceptions Noted
		Observed storage processes to confirm documents and storage media are stored properly in environmentally secure containers.	No Relevant Exceptions Noted

8.2	The system maintains and/or disposes of personnel and payroll records in accordance with government-wide and agency-specific guidelines.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, the system maintains personnel and payroll records in accordance with government-wide and agency-specific guidelines.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that the system is required to maintain personnel and payroll records in accordance with government-wide and agency-specific guidelines.	No Relevant Exceptions Noted
		Observed the personnel and payroll record storage processes to confirm the system maintains personnel and payroll records in accordance with government-wide and agency-specific guidelines.	No Relevant Exceptions Noted
8.3	All visitors to the Payroll Office must sign-in and out with the authorized security personnel.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, visitors to the Payroll Office must sign-in and out with the authorized security personnel.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that visitors to the Payroll Office must sign-in and out with the authorized security personnel.	No Relevant Exceptions Noted
		Scanned visitor log to the payroll office to confirm that visitors must sign-in and with the authorized security personnel.	No Relevant Exceptions Noted
8.4	All terminals and payroll records are located in physically secured locations.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users,	No Relevant Exceptions Noted

		terminals and payroll records are located in physically secured locations.	
		Scanned policies and procedures to confirm that terminals and payroll records are located in physically secured locations.	No Relevant Exceptions Noted
		Toured and observed the terminal rooms to confirm they are physically secure.	No Relevant Exceptions Noted
8.5	Users maintain and/or dispose of personnel and payroll records in accordance with government-wide and agency-specific guidelines.	Confirmed through corroborative inquiry with appropriate payroll office management and functional users, that users maintain and/or dispose of personnel and payroll records in accordance with government-wide and agency-specific guidelines.	No Relevant Exceptions Noted
		Scanned policies and procedures to confirm that users maintain and/or dispose of personnel and payroll records in accordance with government-wide and agency-specific guidelines.	No Relevant Exceptions Noted
		Observed destruction bins to confirm that payroll records are disposed of in accordance with government-wide and agency-specific guidelines.	No Relevant Exceptions Noted

Security Design and Configuration Availability (SDCA)

Control Objective SDCA-1	Control Activity	Test of Controls	Test Results
Procedural Review - An annual IA review is conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations.	DOD and DFAS policy both direct an annual Information assurance review. Review appropriate generated documentation to ensure that these processes are accomplished.	Scanned DECC ME System Readiness Reports (SRR) and corroborated IA reviews for SRR process with Information Assurance Manager. Scanned Residual Risk Assessment for DCPS SSAA re-accreditation and corroborated the review process with DCPS ISSO.	DECC ME – The Risk Assessment has been performed, however it is not in total compliance with DoD 8510.1-M. SRR reviews are regularly performed which may detect non-items that are non-compliant with DISA standards. TSOPE – DCPS does not perform annual Information Assurance reviews. However DCPS is audited each year by various entities and the scope of the reviews materially covers the information required by the objective.

Control Objective SDCA-2	Control Activity	Test of Controls	Test Results
Compliance Testing - A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment.	Procedures addressing the testing of patches, upgrades, and new AIS applications are documented.	Scanned the security test and evaluation guidelines as listed in the DECC ME SSAA and the DCPS SSAA and scanned the Change Management Plan included in the SSAA to confirm test procedures are included in the procedures.	No Relevant Exceptions Noted

Control Objective SDCA-3	Control Activity	Test of Controls	Test Results
Ports, Protocols, and Services - DoD information systems comply with DoD ports, protocols, and services guidance. AIS applications, outsourced IT-based processes and	DECC ME follows the processes and controls enumerated in the STIGs which mirror DoD policy and guidance.	Gathered network traffic through the use of Securify monitoring points positioned on the DISA network and analyzed the network traffic to confirm whether the DCPS ports,	Extraneous services are in operation on all three Logical Partitions and the enclave is not in compliance with the DoD Ports, Protocols and Services guidance. However the risks posed

platform IT identify the network ports, protocols, and services they plan to use as early in the life cycle as possible and notify hosting enclaves. Enclaves register all active ports, protocols, and services in accordance with DoD and DoD Component guidance.		protocols, and services are in accordance with DISA STIGS, DOD Guidance and regulations regarding the appropriate usage of ports protocols and services.	by these services are mitigated by the other security controls in place at DECC ME. Additionally, the application level controls noted elsewhere in this report provide mitigating controls.

Security Design and Configuration Integrity (SDCI)

Control Objective SDCI–1	Control Activity	Test of Controls	Test Results
Control Board - All information systems are under the control of a chartered Configuration Control Board (CCB) that meets regularly. The Information Assurance Manager (IAM) is a member of the CCB.	All changes to information systems at DISA DECC-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 DECC-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. The DISA Executive Software CCB consists of representative of DISA management as well as all the DISA-DECCs. The DISA DECC-ME local CCB consists of all department heads and the Information Assurance Manager (IAM)	Scanned the policies and procedures for the Executive Software Change Control Board (ESCCB) to confirm the ESCCB meets on a weekly basis and minutes are maintained. Inspected a haphazard sample of local CCB meeting notes to confirm the notes include of a list of the open change requests to be discussed or that were discussed at the meeting.	We noted ESCCB meeting notes are not maintained for the weekly meetings and the local CCB charter could not be located Through corroborative inquiry, we noted that major software changes are evaluated by the ESCCB prior to implementation and minor changes and updates are evaluated by the local CCB prior to implementation.

Control Objective SDCI-2	Control Activity	Test of Controls	Test Results
Configuration Specifications - A DoD reference document such as a security technical implementation guide or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products that require use of the product's IA capabilities. If a Departmental reference document is not available, the system owner works with DISA or NSA to draft configuration guidance for inclusion in a DoD reference guide.	DISA has developed and requires compliance with the Security Technical Implementation Guides appropriate to the operating system, application or hardware.	Scanned the appropriate DISA STIGS and configuration documentation to determine compliance with the configuration specifications. Analyzed the gathered network traffic to determine the compliance of the operating system with the specifications.	Although the enclave and the application is in compliance with certain components of the DISA issued STIGs, the enclave and application are not in full compliance with the STIGs. Through our other testing noted throughout this report, we observed there are multiple compensating security controls and application level controls that would mitigate the material risk of these noncompliant items.

Control Objective SDCI-3	Control Activity	Test of Controls	Test Results
Dedicated IA Services - Acquisition or outsourcing of dedicated IA services such as incident monitoring, analysis and response; operation of IA devices, such as firewalls; or key management services are supported by a formal risk analysis and approved by the DoD Component CIO.	Business processes supported by private sector information systems and outsourced information technologies shall be reviewed and managed relative to contributions to mission outcomes and strategic goals and objectives, in accordance with 40 U.S.C. Sections 1423 and 1451. Data shall be collected to support reporting and IA management activities across the investment life cycle.	Inspected appropriate Service Level Agreements to determine the roles and responsibilities of the FSO. Scanned the FSO reports to determine incident monitoring and response, operation of IA devices.	No Relevant Exceptions Noted

Control Objective SDCI-4	Control Activity	Test of Controls	Test Results
Interconnection Documentation - For AIS applications, a list of all (potential) hosting enclaves is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements. For enclaves, a list of all hosted AIS applications, interconnected outsourced IT-based processes, and interconnected IT platforms is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements.	All interconnections of DoD information systems are be managed to continuously minimize community risk by ensuring that the assurance of one system is not undermined by vulnerabilities of interconnected systems	Inspected C4ISP documentation and compared with the information provided in the application SSAA. Analyzed the network traffic gathered by the Securify monitoring point to identify the systems by IP address via the central registry and check the results against the information provided by the application SSO.	Several undocumented interfaces have been observed communicating with DCPS. However, the amount and types of traffic noted do not alone constitute a material level of risk to the application or the enclave. We observed compensating controls such as the intrusion detection systems and the event exception reports that are reviewed by the appropriate managers that mitigate this risk.

Control Objective SDCI-5	Control Activity	Test of Controls	Test Results
Impact Assessment - Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.	All changes made at DISA DECC-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 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.	Inspected the policies and procedures for the ESCCB to confirm changes are assessed for Information Assurance prior to implementation.	Policies and procedures are in place to test changes prior to implementation in the production environment. However, appropriate paperwork documenting the test procedures and results is not maintained. Through corroborative inquiry, we noted testing procedures were performed on the two logical partitions solely dedicated to testing the application and the operating system. Additionally, we inspected documentary evidence that both of the test LPARs are covered by the change control board which does provide some documentation regarding the changes to the test environment.

Control Objective SDCI-6	Control Activity	Test of Controls	Test Results
IA for IT Services - Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities.	The service level agreement (SLA) between DFAS and DISA DECC-ME explicitly states IA roles and responsibilities for both customer and service provider.	Scanned the service level agreement (SLA) between DISA and DFAS to confirm that the agreement defines IA responsibilities for DISA, including: • Protection of all files with approved DISA system security package in coordination with DFAS-HQ; • Security for the MZF environment; • Security for database software; • Providing a physically and environmentally secure facility in accordance with DoD	No Relevant Exceptions Noted

		regulations.	

Control Objective SDCI-7	Control Activity	Test of Controls	Test Results
Non-repudiation - NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards are to be applied as they become available.	DECC ME is in the process of encrypting all data streams to the FIPS-140-2 standard.	Implemented Securify monitoring points at appropriate network nodes to view the network traffic flows to confirm the use of encryption and the appropriate implementation of PKI within the enclave.	DCPS traffic that is transmitted on external networks is encrypted, however, DCPS traffic that is transmitted on internal DoD networks is not encrypted. We observed controls such as authentication mechanisms and intrusion detection systems that mitigate this risk. In addition, the ability to capture, identify, modify, and reinsert unencrypted DCPS data traffic would be technically difficult to accomplish.

Control Objective SDCI-8	Control Activity	Test of Controls	Test Results
Change Management Process - A configuration management (CM) process is implemented that includes requirements for: • Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation; • A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems; • A testing process to verify proposed configuration changes	There is a defined configuration management (CM) process in place at DISA DECC-ME. The process is documented in the SSAA under Appendix S – Change Management Plan. Included in the plan are: • Formally documented CM roles, responsibilities and procedures including management of IA information and documentation; • The detailed role of the Change Control Board (CCB) including its roles for reviewing and approving changes; • The testing process that all changes must go through, including the migration of the	Scanned the Configuration Management policies included in the SSAA. Inspected a haphazard sample of changes to confirm DISA change management processes were followed.	36 of 45 sampled changes were initiated into production by the requestor. Through corroborative inquiry, we determined that all changes must be loaded into the scheduling software in order to be implemented into production. The requestors noted in our exceptions do not have access to the scheduling software. The individuals who perform the scheduling review the change to determine whether it was approved by the CCB. We also noted 5 of 45 sampled changes were documented as having been implemented without testing.

prior to implementation in the operational environment; and • A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.	change from the development region to the testing region, and the testing region to production; • Steps for reviewing the CM process to ensure its operation effectiveness.		However, our subsequent corroborative inquiry of this exception noted that testing had been performed, however, the wrong box in the change management documentation had been completed.

Control Objective SDCI-9	Control Activity	Test of Controls	Test Results
System Library Management Controls - System libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.	The DISA System Support Office (SSO), a unit independent of DECC operations, is responsible for maintaining the system libraries. Access to system libraries is restricted to authorized individuals.	Inspected the Executive Software Plan and observed the system libraries maintenance process to confirm the SSO is maintaining the libraries. Scanned the access list for personnel with access to the system libraries on the MZF LPAR from Information Systems to confirm that access to the system libraries is restricted to the Operating Systems Section personnel.	No Relevant Exceptions Noted

Security Design and Configuration Confidentiality (SDCC)

Control Objective SDCC-1	Control Activity	Test of Controls	Test Results
Acquisition Standards - The acquisition of all IA- and IA-enabled IT products is limited to products that have been evaluated by the NSA or in accordance with NSA-approved processes. The acquisition of all IA- and IA-enabled COTS IT products is limited to products that have been evaluated or validated through one of the following sources – the International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the NIAP Evaluation and Validation Program, or the FIPS validation program. Robustness requirements, the mission, and customer needs will enable an experienced information systems security engineer to recommend a Protection Profile, a particular evaluated product or a security target with the appropriate assurance requirements for a product to be submitted for evaluation.	The SSO is responsible for reviewing and approving all COTS IT products.	Scanned the policies and procedures regarding the acquisition of COTS products to confirm that the DISA SSO reviews all acquisitions that reflect changes to the software baseline.	No Relevant Exceptions Noted

Control Objective SDCC-2	Control Activity	Test of Controls	Test Results
Specified Robustness – At a minimum, medium-robustness COTS IA and IA-enabled products are used to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system. The medium-robustness requirements for products are defined in the Protection Profile Consistency Guidance for Medium Robustness published under the IATF. COTS IA and IA-enabled IT products used for access control, data separation, or privacy on sensitive systems already protected by approved medium-robustness products, at a minimum, satisfy the requirements for basic robustness. If these COTS IA and IA-enabled IT products are used to protect National Security Information by cryptographic means, NSA-approved key management may be required.	Appropriate IA products are implemented to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system.	Implemented Securify monitoring points at appropriate network nodes to view the network traffic flows and to determine what IA and IA enabled products are used to protect sensitive information in transit and at rest.	DCPS traffic that is transmitted on external networks is encrypted, however, DCPS traffic that is transmitted on internal DoD networks is not encrypted. We observed controls such as authentication mechanisms and intrusion detection systems that mitigate this risk. In addition, the ability to capture, identify, modify, and reinsert DCPS data traffic would be technically difficult to accomplish.

Identification and Authentication Integrity (IAC)

Control Objective IAC-1	Control Activity	Test of Controls	Test Results
Group Identification and Authentication - Group authenticators for application or network access may be used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA).	The use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication shall be in accordance with published DoD policy and procedures. These technologies shall be incorporated in all new acquisitions and upgrades whenever possible. Where interoperable PKI is required for the exchange of unclassified information with vendors and contractors, the Department of Defense shall only accept PKI certificates obtained from a DoD-approved external certificate authority or other mechanisms approved in accordance with DoD policy.	Implemented Securify monitoring points at appropriate network nodes to confirm group authenticators for application or network access are only used in conjunction with an individual authenticator.	Our testing noted managers are sharing user IDs in special circumstances. These IDs only have limited access capabilities to perform certain limited payroll functions. Our corroborative inquiry noted the personnel sharing the IDs are authorized to do so and that other mitigating application controls, such as exception reporting, are in place.

Control Objective IAC-2	Control Activity	Test of Controls	Test Results
Individual Identification and Authentication - DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user login ID) and password. For systems utilizing a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive 8-character mix of upper case letters, lower case letters,	DISA user IDs and passwords are configured according to DISA standards.	Implemented Securify monitoring points at appropriate network nodes to confirm system access is gained through the presentation of an individual identifier and password.	Our testing noted managers are sharing user IDs in special circumstances. These IDs only have limited access capabilities to perform certain limited payroll functions. Our corroborative inquiry noted the personnel sharing the IDs are authorized to do so and that other application controls, such as exception reporting, are in place.

numbers, and special characters, including at least one of each. At least four characters must be changed when a new password is created. Deployed/tactical systems with limited data input capabilities implement the password to the extent possible. Registration to receive a user ID and password includes authorization by a supervisor, and is done in person before a designated registration authority. Additionally, to the extent system capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse. All factory set, default or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission.			

Enclave and Computing Environment Availability (ECEA)

Control Objective ECEA-1	Control Activity	Test of Controls	Test Results
Virus Protection - All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates.	Anti-virus software is installed on all PCs, laptops, and systems under DECC-ME control, and application software specific to the customers processing requirements is provided by either commercial vendors or Government CDAs.	Inspected all servers and a haphazard sample of workstations at each site for compliance with virus protection requirements.	No Relevant Exceptions Noted

Enclave and Computing Environment Integrity (ECEI)

Control Objective ECEI-1	Control Activity	Test of Controls	Test Results
Audit Trail, Monitoring, Analysis and Reporting - An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected	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.	Inspected the logs that are maintained (both automated and manual) to confirm that the audit capability is in existence and operating according to specifications.	Audit logs are generated. There is no end user configurable capability to disable the system in the event of an IA violation. Our corroborative inquiry did note that incident response capacities do include active management of the network infrastructure that would enable security and operations personnel to disable a system if an IA violation was detected.

Control Objective ECEI-2	Control Activity	Test of Controls	Test Results
Privileged Account Control - All privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, and web administration). The IAM tracks privileged role assignments.	Access to the system software is administered based on roles.	Inspected a listing of users with access to the operating system software on the MZF LPAR to confirm that access to the datasets is restricted to the Operating Systems Section through comparison to the Organizational Chart.	No Relevant Exceptions Noted
	Access to the Control M scheduler is restricted to appropriate operations personnel.	Inspected a listing of all users with access to Control M on MZF to confirm that each user is a current employee and that access appears reasonable per job function by comparing to the DISA DECC-ME Organizational Chart.	No Relevant Exceptions Noted

Enclave and Computing Environment Confidentiality (ECEC)

Control Objective ECEC–1	Control Activity	Test of Controls	Test Results
Access for Need-to-Know - Access to all DoD information is determined by both its classification and user need-to-know. Need-to-know is established by the Information Owner and enforced by discretionary or role-based access controls.	Access to all DoD information systems is based on a demonstrated need-to-know, and granted in accordance with applicable laws and DoD 5200.2-R for background investigations, special access and IT position designations and requirements.	Scanned the DCPS SSAA to confirm that access to DCPS is unclassified and that users must have a need-to-know to obtain access.	No Relevant Exceptions Noted

Control Objective ECEC–2	Control Activity	Test of Controls	Test Results
Logon - Successive logon attempts are controlled using one or more of the following: • Access is denied after multiple unsuccessful logon attempts; • The number of access attempts in a given period is limited; • A time-delay control system is employed. If the system allows for multiple-logon sessions for each user ID, the system provides a capability to control the number of logon sessions.	CA ACF2 is maintained at both DISA ME and the various payroll offices by a series of security administrators with differing roles (administration, user accounts etc.) The logs are centrally reviewed at DISA ME. Multiple unsuccessful login attempts result in the account being locked. If the account is unused for a specified period then the account is deactivated.	Scanned the weekly reports of access denial and observed one of the security administrators at DISA ME performing three invalid attempts to login and then one attempt to use a valid password.	Password configuration does not comply with DoD 8500.2 requirements. However there are additional compensating controls such as password generational controls, password complexity factors, and multiple levels of access that mitigate this exception.

Control Objective ECEC–3	Control Activity	Test of Controls	Test Results
Least Privilege - Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to	Privilege accounts are only used by DECC ME and DCPS personnel to create/modify/delete user accounts.	Inspected privilege account usage logs to confirm accounts only used to perform create/modify/delete user accounts.	No Relevant Exceptions Noted

privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization.			

Control Objective ECEC–4	Control Activity	Test of Controls	Test Results
Marking and Labeling - Information and DoD information systems that store, process, transit, or display data in any form or format that is not approved for public release comply with all requirements for marking and labeling contained in policy and guidance documents, such as DOD 5200.1R. Markings and labels clearly reflect the classification or sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions.	Information on DoD systems that store, process, transit, or display data in any format that is not approved for public release complies with DoD policy.	Inspected the DISA DECC-ME data center, including onsite tape storage areas, to confirm that labels indicating classification level are affixed to all computers and storage devices.	No Relevant Exceptions Noted

Control Objective ECEC–5	Control Activity	Test of Controls	Test Results
Conformance Monitoring and Testing - Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, and conducted. Testing is intended to ensure that the	DECC ME performs monthly vulnerabilities scans. DCPS system and hardware are reviewed by an FSO SRR.	Inspected periodic vulnerability scans and documentation of system reviews to confirm conformance monitoring is in effect.	No Relevant Exceptions Noted

system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.			

Control Objective ECEC–6	Control Activity	Test of Controls	Test Results
Warning Message - All users are warned that they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing.	All DISA networks and platforms present a message to users upon logon, which warns them that they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing.	Observed Security Systems Specialist login into the DISA network and then into the DCPS. Inspected the text from the login to confirm warning message appears upon login.	No Relevant Exceptions Noted

Control Objective ECEC–7	Control Activity	Test of Controls	Test Results
Account Control - A comprehensive account management process is implemented to ensure that only authorized users can gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.	User account are suspended after 30 days of no activity, (60 days for TSO and Payroll offices) and removed after 90 days. Accounts are issued by local security administrators, User access administration controls are tested in multiple sections of this report, including sections APP, IAC, ECEI, ECEC, and EBDC.	User access administration is tested in several areas in this report. Scanned logs of suspended accounts and removed accounts to confirm inactive/terminated/ transferred user accounts are removed.	No Relevant Exceptions Noted

Enclave Boundary Defense Availability (EBDA)

Control Objective EBDA-1	Control Activity	Test of Controls	Test Results
VPN Controls - All VPN traffic is visible to network intrusion detection systems (IDS).	ISS Real Secure is installed at various points that give visibility into the network traffic ingressing and egressing the enclave.	Inspected the technical capabilities and actual data streams to confirm that the ISS monitors are capable of viewing VPN traffic.	No Relevant Exceptions Noted

Enclave Boundary Defense Confidentiality (EBDC)

Control Objective EBDC-1	Control Activity	Test of Controls	Test Results
Boundary Defense - Boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, at layered or internal enclave boundaries and at key points in the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or technical means.	Perimeter firewalls and intrusion detection systems are implemented.	Implemented Securify monitoring points at appropriate network nodes to confirm the behavior of the traffic consistent with firewall rules and behaviors. Observed that an intrusion detection system has been implemented.	No Relevant Exceptions Noted

Control Objective EBDC-2	Control Activity	Test of Controls	Test Results
Public WAN Connection - Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a demilitarized zone (DMZ).	DoD information systems shall regulate remote access and access to the Internet by employing positive technical controls such as proxy services and screened subnets, also called demilitarized zones (DMZ), or through systems that are isolated from all other DoD information systems through physical means.	Scanned the network diagrams for the presence of a DMZ with regards to traffic that may flow into commercial wide area networks (i.e. the internet). Implemented Securify monitoring points at appropriate network nodes to view the network traffic flows and confirm the use of a DMZ	No Relevant Exceptions Noted

Control Objective EBDC-3	Control Activity	Test of Controls	Test Results
Remote Access for Privileged Functions - Remote access for privileged functions is discouraged, is permitted only for compelling	There is a remote dial-in router provided for Systems Administrators which requires Secure Shell restrictions. ESM is installed on a	Inspected the presence of remote access for privileged functions to confirm that remote access contain security measures such as a complete	No Relevant Exceptions Noted

operational needs, and is strictly controlled. In addition to EBRU-1, sessions employ security measures, such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the IAM/O reviews the log for every remote session.	some of these systems.	audit trail and the presence of additional security controls such as VPN with blocking mode, strong encryption, strong passwords or other means of authentication are present and operating.	

Control Objective EBDC-4	Control Activity	Test of Controls	Test Results
Remote Access for User Functions - All remote access to DoD information systems, to include telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Remote access always uses encryption to protect the confidentiality of the session. The session level encryption equals or exceeds the robustness established in ECCT. Authenticators are restricted to those that offer strong protection against spoofing. Information regarding remote access mechanisms (e.g., Internet address, dial-up connection telephone number) is protected.	Remote access to the Internet is regulated by positive technical controls such as proxy services and screened subnets, also called demilitarized zones (DMZ), or through systems that are isolated from all other DoD information systems through physical means.	Implemented Securify monitoring points at appropriate network nodes to confirm appropriate strength encryption established in ECCT and to identify and document additional controls regarding internet address, dial-up connection telephone numbers etc.	Our testing noted that remote access is not authenticated via a DMZ. However, as a compensating control, all authentication is performed via an approved security application, with a FIPS 140-2 compliant encryption algorithm with a secondary authentication required by the application.

Physical and Environmental Availability (PEA)

Control Objective PEA-1	Control Activity	Test of Controls	Test Results
Environmental Controls - Appropriate fire detection & suppression, humidity, temperature, and emergency cut-off controls have been implemented and functioning properly	The DISA DECC-ME has implemented fire detection and suppression systems, humidity and water monitors, temperature monitors and emergency cut-off controls.	Inquired with Public Works that the DISA DECC-ME data center is equipped with fire detection monitors, a fire suppression system, temperature monitors, humidity monitors and an emergency cut-off switch. Observed the data center to observe and confirm the existence and operation of the environmental controls.	No Relevant Exceptions Noted

Physical and Environmental Confidentiality (PEC)

Control Objective PEC-1	Control Activity	Test of Controls	Test Results
Clearing and Sanitizing - All documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released outside of the Department of Defense according to DoD 5200.1-R and ASD(C3I) Memorandum, dated June 4, 2001, subject: "Disposition of Unclassified DoD Computer Hard Drives."	All documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released, and sign off is required to certify the destruction of such media.	Observed the DISA DECC-ME hard drive sanitizing procedures with the DISA DECC-ME Information Assurance Manager.	No exceptions noted

Control Objective PEC-2	Control Activity	Test of Controls	Test Results
Physical Protection of Facilities - Every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release is controlled during working hours and guarded or locked during non-work hours.	All DISA facilities at DISA DECC-ME are locked at all times. Access is restricted using proximity cards, with PIN technology, which are controlled and issued by the Security Manager.	Observed the physical access controls in place at DISA DECC-ME to determine that appropriate physical access restrictions are in place.	No Relevant Exceptions Noted

Control Objective PEC-3	Control Activity	Test of Controls	Test Results
Physical Security Testing - A facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate key computing facilities.	The Naval Inventory Control Point conducts periodic, unannounced penetration testing to confirm that physical security is adequate.	Inquired with Chief of Police, Naval Inventory Control Point (NAVICP), and Security Director – NAVICP, that at least once every 3 years, NAVICP is subjected to an unannounced penetration attempt by the Joint Chiefs Vulnerability Assessment	No Relevant Exceptions Noted

		Team.	
	DISA DECC-ME's SSAA requires the performance of physical security inspections by the Security Office.	Scanned the DISA DECC-ME System Security Authorization Agreement (SSAA) to determine that section 6.4.2 requires that physical security inspections be conducted by the Security Office as a component of Traditional Security.	No Relevant Exceptions Noted

Control Objective PEC-4	Control Activity	Test of Controls	Test Results
Workplace Security Procedures - Procedures are implemented to ensure the proper handling and storage of information, such as end-of-day security checks, unannounced security checks, and, where appropriate, the imposition of a two-person rule within the computing facility.	Procedures are in place to ensure that documents and electronic media are stored in accordance with DoD standards.	Scanned the DISA DECC-ME SSAA Appendix J, System Rules of Behavior to determine that all government owned property leaving the data center building is inspected. Toured the data center facility and observed that access to storage areas is controlled through the use of proximity cards, PINs, and closed circuit TV.	No Relevant Exceptions Noted

Control Objective PEC-5	Control Activity	Test of Controls	Test Results
Storage - Documents and equipment are stored in approved containers or facilities with maintenance and accountability procedures that comply with DoD 5200.1-R.	All documents and storage media are stored in physically and environmentally secure containers.	Scanned the DISA DECC-ME SSAA to determine that the compute facility of the data center building has been approved as a Collateral Classified Storage Area up to the Secret level. Toured the data center facility and observed that access to storage areas is controlled through the use of proximity cards, PINs, and closed circuit TV.	No Relevant Exceptions Noted

Control Objective PEC-6	Control Activity	Test of Controls	Test Results
Visitor Control to Computing Facilities - Current signed procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility.	The DISA DECC-ME SSAA requires all uncleared personnel to be escorted at all times while inside the DISA DECC-ME (Building 308).	Scanned the DISA DECC-ME System Security Authorization Agreement (SSAA) to determine that it requires that appropriately cleared personnel must escort all uncleared personnel in the DISA DECC-ME.	No Relevant Exceptions Noted
	All visitors to the DISA DECC-ME must sign-in and out with the guard on duty.	Inspected the visitors sign-in at the DISA DECC-ME determine that visitors are required to exchange their normal employee or visitor badges for special DISA DECC-ME badges and sign visitor's log.	No Relevant Exceptions Noted

Personnel Availability (PA)

Control Objective PA-1	Control Activity	Test of Controls	Test Results
Security Rules of Behavior or Acceptable Use Policy - A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access.	The DISA DECC-ME SSAA includes an Appendix J, System Rules of Behavior, which describes the IA operations of the DoD information system and clearly delineates IA responsibilities and expected behavior of all personnel.	Scanned the DISA DECC-ME System Security Authorization Agreement (SSAA), Appendix J, System Rules of Behavior to determine that it includes a Systems Security Plan.	No Relevant Exceptions Noted

Personnel Integrity (PI)

Control Objective PI-1	Control Activity	Test of Controls	Test Results
Information Assurance Training 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.	The DECC ME SSAA includes an Appendix J, System Rules of Behavior, which describes the IA operations of the DoD information system and clearly delineates IA responsibilities and expected behavior of all personnel.	Scanned training documentation provided by the DISA DECC-ME Security Officer to determine that new employees go through security awareness training their first day and there is an annual refresher course. Scanned the DCPS SSAA to determine that the Pensacola TSO has created an online security training awareness program that is required to be completed before a DCPS account.	No Relevant Exceptions Noted
	DECC ME has ongoing security awareness programs that include initial training and periodic refresher training.	Scanned training documentation provided by the DECC ME Security Officer to determine that new employees go through security awareness training their first day and there is an annual refresher course.	No Relevant Exceptions Noted

Personnel Confidentiality (PC)

Control Objective PC-1	Control Activity	Test of Controls	Test Results
Accesses to Information - Individuals requiring access to sensitive information are processed for access authorization in accordance with DoD personnel security policies.	The DISA DECC-ME 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 DISA DECC-ME employees (military, civilian or contractors) will have a SECRET security clearance and a favorably completed NAC.	Selected a haphazard sample of employees with highly permissive access to the facilities at DISA DECC-ME and inspected their clearance levels in the Defense Clearance Investigation Index with the DISA DECC-ME Security Officer to confirm that level security clearance level is appropriate.	No Relevant Exceptions Noted

Control Objective PC-2	Control Activity	Test of Controls	Test Results
Maintenance Personnel - Maintenance is performed only by authorized personnel. The processes for determining authorization and the list of authorized maintenance personnel are documented.	The DISA DECC-ME SSAA requires that most maintenance and all cleaning personnel are required to have at least a Secret clearance to work in building 308. If they do not have the appropriate clearance they will be escorted at all times.	Inquired with the DISA DECC-ME Security Officer and Information Assurance Manager to determine that maintenance personnel are vetted just like any other employee or contractor.	No Relevant Exceptions Noted

Control Objective PC-3	Control Activity	Test of Controls	Test Results
Access to Need-to-Know Information - Only individuals who have a valid need-to-know that is demonstrated by assigned official Government duties and who satisfy all personnel security criteria (e.g., IT	The DISA DECC-ME SSAA requires that Access to all DoD information systems shall be based on a demonstrated need-to-know, and granted in accordance with applicable laws and	Selected a haphazard sample of employees with highly permissive access to the facilities at DISA DECC-ME and inspected their clearance levels in the Defense Clearance Investigation Index with	No Relevant Exceptions Noted

position sensitivity background investigation requirements outlined in DoD 5200.2-R) are granted access to information with special protection measures or restricted distribution as established by the information owner.	DoD 5200.2-R for background investigations, special access and IT position designations and requirements. An appropriate security clearance and non-disclosure agreement are also required for access to classified information in accordance with DoD 5200.1-R.	the DISA DECC-ME Security Officer to confirm that level security clearance level is appropriate.	

Vulnerability and Incident Management Availability (VIMA)

Control Objective VIMA-1	Control Activity	Test of Controls	Test Results
Vulnerability Management - A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention	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 the checklists have been applied from the STIG and the vulnerability alerts have been installed, a security readiness review (SRR) and an ISS scan will be conducted of the operating system. Security assessments that require a scan will use the Internet Security Scanner (ISS) and the FSO Full Scan Policy. The scan will be conducted using a direct connection from the	Scanned the most recent reports from the VMS that pertain specifically to DCPS and inspected the patch levels to identify mitigation techniques. Implemented Securify monitoring points at appropriate network nodes to confirm STIG compliance with vulnerability requirements. Scanned recent SRR reports to confirm SRRs are performed.	No Relevant Exceptions Noted

and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of Vulnerabilities.	system running ISS to the system being assessed or the site is authorized to connect the asset to an isolated network during the ISS scan. Each site will place their self-assessment in the Security Readiness Review Database (SRRDB). If the systems have a database, web server, or any other software that has a STIG, they must go through a FSO SRR and the results put in the self-assessment of the SRR database.		

Section IV: Supplemental Information Provided by DFAS and DISA

IV. Supplemental Information Provided by DFAS and DISA

Introduction

This section has been prepared by DFAS and DISA and is included to provide user organizations with information DFAS and DISA believes will be of interest to such organizations but which is not covered within the scope or control objectives established for the SAS 70 review. Specifically included is a summary of procedures that DFAS and DISA have put into place to enable recovery from a disaster affecting the DFAS TSOPE and the DISA DECC at Mechanicsburg, PA.

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, and accordingly, the Office of Inspector General 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 there is a disaster or impending threat that would render DCPS production support inoperable (e.g., hurricane, damage to TSOPE facilities due to fire, etc.). This plan is evaluated and updated, accordingly, on an annual basis. In the impending threat or event, production support control for the DCPS production support is transferred to an alternate-processing site, currently defined to be DAC Huntsville, AL. Contained in the detailed COOP are names of DCPS staff members who will serve as a pool of resources to be mobilized to execute the plan and a list of documentation and supplies that are necessary to support the mobilized team.

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

DISA DECC-ME Business Continuity Plans

To accommodate a major disaster at any major DISA processing center, DISA has established the DISA Continuity and Test Facility (DCTF) at Slidell, LA. This facility is equipped with computational, DASD (Direct Access Storage Device), and telecommunications resources sized to provide a fully functional host site with the capacity to support a major disaster at any DISA processing center. The COOP support agreement between DFAS as the customer and DISA as the provider of processing system and communications services provides for restoring host site processing in the event of a major disaster and 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 OS/390 operating system, the DCPS IDMS database, and related mid-tier servers and communication devices. Backup tapes containing the incremental daily and the complete weekly backups are rotated off site to the DISA DECC Detachment at Chambersburg, PA for storage on a predetermined schedule.

The Crisis Management Team (CMT) at DECC-ME is responsible for declaring a disaster has occurred and initiate the BCP. The CMT will then activate the following response teams: Communications Team (COMT), Recovery Coordination Team (RCT), Site Recovery Team (SRT), and the Crisis Support Team (CST). 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. TSOPE personnel participate in the yearly COOP test to ensure that the process works correctly and documentation is updated appropriately.

On September 12, 2004, Hurricane Ivan caused damage to the DFAS payroll office at the Pensacola Naval Air Station and the TSOPE facility at Saufley Field in Pensacola. As a result, DFAS management implemented the COOPs for the payroll office and TSOPE operations. The implementation of COOP activities allowed DFAS to successfully run civilian payroll for all of its customers on time from an alternative operating location. TSOPE returned to operation on September 24, 2004.

Acronyms and Abbreviations

ACF2	Access Control Facility 2
ACL	Audit Command Language
BMMP	Business Management Modernization Program
BPH	Business Process Handbook
C2M	Continuous Compliance Model
CCB	Configuration Control Board
CDA	Central Design Agency
CM	Configuration Management
CONUS	Continental United States
COOP	Continuity of Operations
COR	Contracting Officer Representative
COTS	Commercial Off The Shelf
CRC	Cyclic Redundancy Check
CSR	Customer Service Representatives
DAA	Designated Approving Authority
DAPS	Defense Automated Printing Service
DCPS	Defense Civilian Pay System
DECC	Defense Enterprise Computing Center
DECC-ME	Defense Enterprise Computing Center - Mechanicsburg
DFAS	Defense Finance and Accounting Service
DFAS-HQ	Defense Finance and Accounting Service-Headquarters
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DMZ	Demilitarized Zone
DNS	Domain Name Server
DoD	Department of Defense
DoDFMR	Department of Defense Financial Management Regulations
DoDI	Department of Defense Instruction
DOE	Department of Energy
DPAS	Defense Property Accountability System
ESCCB	Executive Software Change Control Board
FFMIA	Federal Financial Management Improvement Act
FISCAM	Federal Information Systems Controls Audit Manual
FISMA	Federal information Security Management Act
FSO	Field Security Operations
GAGAS	Generally Accepted Government Auditing Standards
GAO	General Accounting Office
GOTS	Government - Off – The – Shelf - Application

IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IATF	Information Assurance Technical Framework
IDS	Intrusion Detection System
IG DOD	Inspector General Department of Defense
IP	Internet Protocol
ISSO	Information Systems Security Officer
IW	Information Warfare
LAN	Local Area Network
LES	Leave and Earnings Statements
MAC	Mission Assurance Category
MER	Master Employee Record
NAC	National Agency Check
NAVICP	Naval Inventory Control Point
NES	Navy Enlisted System
NIPRNET	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OIG	Office of the Inspector General
OS	Operating System
PKE	Public Key Enabling
PKI	Public Key Infrastructure
RFQ	Request for Quotation
SAS	Statement on Auditing Standards
SLA	Service Level Agreement
SNA	Systems Network Architecture
SOP	Standard Operating Procedure
SOW	Statement of Work
SRR	System Readiness Report
SSAA	System Security Authorization Agreement
SSO	System Support Office
STIGs	Security Technical Implementation Guidelines
TASO	Terminal Area Security Officer
TSO	Technology Services Organization
TSOPE	Technology Services Engineering Organization in Pensacola
VIS	Vendor Integrity Statement

Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)
Director, Program Analysis and Evaluation

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Combatant Command

Inspector General, U.S. Joint Forces Command

Other Defense Organizations

National Security Agency
Defense Finance and Accounting Service
Inspector General, Defense Information Systems Agency
Director, Defense Logistics Agency
Inspector General, US Joint Forces Command

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 Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
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, in conjunction with contract auditors from Deloitte and Touché and Urbach Kahn and Werlin and the Technical Assessment Division of the Office of the Inspector General of the Department of Defense (IG DoD), prepared this report. Personnel of the Quantitative Methods Division, IG DoD, also contributed to the report.