
July 7, 2005



Information Technology Management

Report on Defense Property
Accountability System Controls
Placed in Operation and Test of
Operating Effectiveness for the
Period September 1, 2004 through
April 30, 2005
(D-2005-092)

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

July 7, 2005

MEMORANDUM FOR THE OFFICE OF THE UNDER SECRETARY OF DEFENSE,
ACQUISITION, TECHNOLOGY, AND LOGISTICS
UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF
FINANCIAL OFFICER
DEPUTY CHIEF FINANCIAL OFFICER
DEPUTY COMPTROLLER (PROGRAM/BUDGET)
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
COMMANDING OFFICER, NAVAL SUPPLY INFORMATION
SYSTEMS ACTIVITY

SUBJECT: Report on the Defense Property Accountability System Controls Placed in
Operation and Test of Operating Effectiveness for the Period September 1, 2004
through April 30, 2005 (Report No. D-2005-092)

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) 428-1054 (DSN 328-1054) or Yolanda C. Watts at (703) 428-1071 (DSN 328-1071). The audit team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:


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

Table of Contents

Foreward	i
Section I	
Independent Service Auditor’s Report.....	1
Section II	
Description of the Defense Property Accountability System Operations and Controls Provided by the Defense Finance and Accounting Service, the Defense Information Systems Agency, and the Naval Supply Information Systems Activity.....	7
Section III	
Control Objectives, Control Activities, and Tests of Operating Effectiveness.....	29
Section IV	
Supplemental Information Provided by the Defense Information Systems Agency.....	103
Acronyms and Abbreviations	107
Report Distribution	109

FOREWORD

This report is intended solely for use by management of the Defense Finance and Accounting Service (DFAS), Defense Information Systems Agency (DISA), and Naval Supply Information Systems Activity (NAVSISA), the Defense Property Accountability System (DPAS) user organizations, and the independent auditors of such user organizations. Department of Defense personnel who manage and use the DPAS will also find this report of interest as it contains information about DPAS general and application controls.

The Department of Defense Office of Inspector General (DoD OIG) is implementing a long-range strategy to conduct audits of DoD financial statements. The Chief Financial Officer's Act of 1990 (P.L. 101-576), as amended, mandates that agencies prepare and conduct audits of financial statements. The reliability of information in DPAS directly impacts DoD's ability to produce reliable, and ultimately auditable, financial statements; which is key to achieving the goals of the Chief Financial Officer's Act.

DPAS provides financial reporting capability for capital assets (assets with a value greater than \$100,000), and asset accountability for more than 10.6 million property assets (assets with a value less than \$100,000) valued at approximately \$48.3 billion as of February 2005. DPAS provides standard general ledger accounting in conformance with the United States Government Standard General Ledger (USSGL) at the transaction level and subsidiary reporting for capital assets. DPAS tracks accountability for various types of property including personal property, real property, and heritage assets. DPAS has security features that provide asset visibility at many levels based on users' roles and needs.

This audit assessed controls over DPAS accountability of assets totaling approximately \$48.3 billion. This report provides an opinion on the fairness of presentation, the adequacy of design, and the operating effectiveness of key controls that are relevant to audits of user organization financial statements. As a result, this audit precludes the need for multiple audits of DPAS controls previously performed by user organizations to plan or conduct financial statement and performance audits. This audit will also provide, in a separate audit report, recommendations to management for correction of identified control deficiencies. Effective internal control is critical to achieving reliable information for all management reporting and decision making purposes.

Section I: Independent Service Auditors' Report



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

July 7, 2005

MEMORANDUM FOR THE OFFICE OF THE UNDER SECRETARY OF DEFENSE,
ACQUISITION, TECHNOLOGY, AND LOGISTICS
UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF
FINANCIAL OFFICER
DEPUTY CHIEF FINANCIAL OFFICER
DEPUTY COMPTROLLER (PROGRAM/BUDGET)
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
COMMANDING OFFICER, NAVAL SUPPLY INFORMATION
SYSTEMS ACTIVITY

SUBJECT: Report on the Defense Property Accountability System Controls Placed in
Operation and Test of Operating Effectiveness for the Period September 1, 2004
through April 30, 2005

We have examined the accompanying description of the general computer and application controls related to DPAS (Section II) of this report. The DPAS program is overseen and managed by the Office of the Under Secretary of Defense, Acquisition, Technology and Logistics and used by 329 user groups throughout the Department of Defense (DoD). The DPAS system, including general computer and application controls, is directly supported and maintained by DFAS, DISA, and NAVSISA. 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, DISA, and NAVSISA that may be relevant to a DPAS user organizations' internal controls as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description if those controls were complied with satisfactorily and user organizations applied those aspects of internal control contemplated in the design of the controls at DFAS, DISA, and NAVSISA; and (3) such controls had been placed in operation as of April 30, 2005.

The control objectives were specified by DoD OIG and accepted by DFAS, DISA and NAVSISA. 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.

DPAS was used by the Army, Navy, and Defense Agencies, including the National Security Agency (NSA). The NSA had its own separate version of DPAS since its property information was classified. In addition, the Navy used DPAS in a manner that is different than the way DPAS is used by the Army and Defense Agencies. The accompanying description includes

includes only those general computer and application control objectives and related control activities related to the nonclassified and non-Navy DPAS versions of the system. DPAS interfaced with over 28 DoD systems that either received data from or transmitted data to DPAS. The accompanying description includes only those general computer and application controls related to the input and output processing of these data files and does not include general computer and application controls over the source and destination systems that send data files to or receive data files from DPAS. Finally, the accompanying description includes only those application controls that were centrally managed and maintained by DFAS, DISA, and NAVSISA and does not include the application controls resident at DPAS user locations. Therefore, our examination did not extend to the general computer and application controls related to the classified and Navy versions of DPAS, the general computer and application controls over the source and destination systems that interfaced with DPAS, or the application controls resident at DPAS user locations.

Our examination was conducted for the purpose of forming an opinion on the description of the DPAS general computer and application controls at DFAS, DISA, and NAVSISA (Section II and the control activities described in Section III of this report). Information about business continuity plans and procedures at DISA, as provided by that organization 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, DISA, and NAVSISA. 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, DISA, and NAVSISA related to their business continuity plans and procedures. Accordingly, we express no opinion on the description of the business continuity plans and procedures provided by DISA.

In our opinion, the accompanying description of the general computer and application controls at DFAS, DISA, and NAVSISA related to DPAS (Section II) presents fairly, in all material respects, the relevant aspects of the controls at DFAS, DISA, and NAVSISA that had been placed in operation as of April 30, 2005. Also, in our opinion, the controls, as described, were 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, DISA, and NAVSISA.

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 September 1, 2004, to April 30, 2005. 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 DPAS 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.

A number of controls in place to ensure compliance with DoD information assurance policies, including DoDI 8500.2 and DoD Information Technology Security Certification and Accreditation Process (DITSCAP) appear to be suitably designed, but our tests of operating

effectiveness indicated inconsistencies in adherence to these policies. In performing our examination, we identified the following deficiencies relating to the operating effectiveness of controls in operation for the period September 1, 2004, to April 30, 2005:

- DISA recorded the system audit trails generated by DPAS. However, DISA did not proactively monitor DPAS system audit trails. As a result, DPAS's controls did not provide reasonable assurance that the following control objectives were fully achieved during the period from September 1, 2004 to April 30, 2005:
 - "Tools are available for the review of audit records and for report generation from audit records" (general computer control objective 34);
 - "Policies and techniques have been implemented for using and monitoring the use of system utilities" (general computer control objective 72); and
 - "Installation of system software is documented and reviewed" (general computer control objective 74).
- DISA had documented standard operating procedures covering the DPAS-related operations at DISA Ogden. However, those standard operating procedures were outdated and incomplete. As a result, DPAS's controls did not provide reasonable assurance that the following control objectives were fully achieved during the period from September 1, 2004 to April 30, 2005:
 - "Policies and techniques have been implemented for using and monitoring the use of system utilities" (general computer control objective 72) and
 - "Formal procedures guide personnel in performing their duties" (general computer control objective 80).
- DISA performed certain procedures to process and monitor system transaction files, as well as certain procedures to correct errors and problems associated with transaction file processing. However, those procedures were not documented. In addition, the majority of the transaction processing, monitoring, and error correction functions were performed by one individual at DISA who was the only person who had the full technical knowledge of DPAS to perform all of the functions. The unavailability of this person could impact the timeliness and quality of system transaction file processing. As a result, DPAS's controls did not provide reasonable assurance that the following control objective was fully achieved during the period from September 1, 2004 to April 30, 2005: "Controls provide reasonable assurance that erroneous transactions are identified without being processed and without undue disruption of the processing of other valid transactions," (application control objective 11).
- DISA performed vulnerability testing to identify DPAS's architecture vulnerabilities. However, DISA did not perform periodic network penetration testing. As a result, DPAS's controls did not provide reasonable assurance that the following control objective was fully achieved during the period from September 1, 2004 to April 30, 2005: "Conformance testing that includes periodic, unannounced, in-depth monitoring and

“Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures is planned, scheduled, and conducted,” (general computer control objective 48).

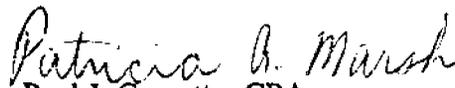
In our opinion, except for the matters described in the preceding paragraphs, the controls that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section III were achieved during the period from September 1, 2004 to April 30, 2005. 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, DISA, and NAVSISA 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, DISA, and NAVSISA is as of April 30, 2005, and information about tests of their operating effectiveness covers the period from September 1, 2004 to April 30, 2005. 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, DISA, and NAVSISA 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 DFAS, DISA, and NAVSISA, the DPAS user organizations, and the independent auditors of such user organizations.

By direction of the Deputy Inspector General for Auditing:


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

**Section II: Description of Defense Property Accountability System
Operations and Controls Provided by the Defense Finance and
Accounting Service, the Defense Information Systems Agency, and
the Naval Supply Information Systems Activity**

II. Description of the Defense Property Accountability System Operations and Controls Provided by the Defense Finance and Accounting Service, Defense Information Systems Agency, and Naval Supply Information Systems Activity

A. Overview of DPAS

History

The Under Secretary of Defense (Comptroller) and the Assistant Secretary of Defense for Command, Control, Communication and Intelligence designated DPAS as a migratory system in Fiscal Year 1995 to bring DoD real and personal property assets under proper accountability and financial control. At that time, DoD real and personal property were considered high-risk areas by the audit community. DoD activities began migrating data to DPAS in 1995. By 2001, DPAS was nearly fully deployed throughout DoD. The Army, Navy, Marine Corps and 22 Defense Agencies adopted DPAS; the Air Force did not. DPAS is considered a legacy system that will be replaced by 2012 as part of Enterprise Resource Plan initiatives at the Army, Navy, Marine Corps, and Defense Logistics Agency. An acquisition strategy is currently being developed to determine the appropriate modernization strategy for DPAS. DPAS is administered by the Under Secretary of Defense (Comptroller) and the Office of the Under Secretary of Defense, Acquisition, Technology and Logistics.

System Capabilities

DPAS provides financial reporting capability for capital assets (assets with a value greater than \$100,000), and asset accountability for more than 10.6 million property assets (assets with a value less than \$100,000) valued at approximately \$48.3 billion as of February 2005. DPAS provides standard general ledger accounting in conformance with the USSGL at the transaction level and subsidiary reporting for capital assets. DPAS tracks accountability for various types of property, including personal property, real property, and heritage assets. DPAS has security features that provide asset visibility at many levels based on users' roles and needs.

DPAS provides DoD users with full support for property accountability, management, and financial reporting. Specifically, it provides the capability to update item authorizations, perform asset cataloging actions, assign accountability, perform accountable record processing (such as receipts, turn-in, transfers, and inventory tracking and status), account for government furnished property, compute depreciation, generate general ledger transactions, update subsidiary and general ledger records, report financial status, maintain an

automated document register, and report disposals. DPAS also supports various maintenance requirements including tracking preventive maintenance schedules and actions, generating work orders, and tracking warranty, loan and lease data. DPAS users have the ability to choose the DPAS functionality they want to use to meet their property accountability needs. In addition to standard reporting capabilities, DPAS provides users with commercially developed ad hoc query and report writing software. This toolset allows DPAS users to create and save custom queries and reports to meet any special reporting requirements that the standard DPAS reports do not support.

System Interfaces

DPAS's primary interface is keyboard input using the Government off-the-Shelf (GOTS) client/server software provided to its users. The majority of the inputs are real-time with the updates being performed immediately. In the instance of batch processing, users generate "Batch Requests" real-time which are then stored in a database table for subsequent processing during the batch cycle. Validation of the real-time input is performed by the client software whenever possible. Should the validation require cross-validation with other table data not resident within the window, the validation will occur within the server software prior to processing. The GOTS software provides users update processes, ad hoc query processes and standard reports.

DPAS has one internal interface that uses DPAS-developed software to accept inventory data generated by Portable Data Collection Devices (PDCDs), also referred to as scanners. Users export a file from their terminal to the PDCD that contains information about inventories to be conducted. Upon completion of the inventories, the results are exported from the PDCD back to the user's terminal. From the user's terminal, the DPAS client software updates user databases. Some PDCDs may be capable of communicating wirelessly. In those instances, the PDCD is configured to communicate with DPAS client software, which in turn processes the updates on a near real-time basis.

With the exception of the Unit Level Logistics System – Supply (ULLS-S4), which is a PC-based self-contained application that uses a floppy diskette, or other similar media, all external interfaces use File Transfer Protocol/Secure File Transfer Protocol to communicate with DPAS. DPAS interfaces with 26 external systems. All interfaces are documented with a service level agreement that contains contact information, data file layouts, file transmission procedures, and frequency of transmission information. With the exception of ULLS-S4, Army Material Command Installation Supply System, and Standard Army Retail Supply System, all interfaces are managed by the DISA DPAS operations support team.

In addition to system interfaces, there are data flows between various DPAS

modules. To build a property record, data is initially entered using the Catalog module with each distinct asset being catalogued with a Stock Number. The Catalog module maintains management data pertaining to the asset with that data flowing from the Catalog module to the Authorization and Document Register modules. The Document Register assigns document numbers, updates status, closes completed actions, and provides visibility for open and closed actions. The Authorization Module feeds data to the Hand Receipt module to provide a link between assets on-hand and the authorization to obtain, retain or turn-in an asset. The Hand Receipt module provides the capability to process all actions that affect asset balances. The Hand Receipt module creates accounting transactions when gains or losses for capital assets occur and feeds data to the Accounting Module generating asset expense and depreciation data. The Hand Receipt also provides data to the Maintenance and Utilization module.

External interfaces are grouped by function as follows:

- *Accounting* - Accounting information, including depreciation data, are interfaced from the DPAS database to selected accounting management systems. The accounting interface is a one-way outbound interface that provides capital asset general ledger and accounting information to cost accounting systems such as Standard Industrial Fund System, Defense Business Management System, Financial Accounting and Management Information System, Washington Headquarters Services Allotment Accounting System, Logistics Modernization Program, and Electronic Business. These interfaces typically occur daily with data sent to the accounting system when there is accounting transaction activity. Plans are under way to add additional accounting interfaces with the Defense Working Capital Accounting System; Standard Accounting and Reporting System; Standard Accounting, Budget, and Reporting System; and Defense Corporate Database.
- *Authorization* - The authorization interface is a one-way inbound interface that supports Army DPAS users by providing equipment authorization requirements from the Logistics Army Authorization Document System. The Logistics Army Authorization Document System data provides users with current and projected equipment requirements. Users review this data to determine whether there is sufficient equipment on-hand to fulfill their mission, when to submit requisitions to cover equipment shortages, and when to initiate turn-in actions for excess equipment. The Logistics Support Activity within the Department of the Army is responsible for sending the file containing Logistics Army Authorization Document System data.
- *Asset Visibility* - Asset visibility interfaces are one-way outbound interfaces that provide data extracts of asset information based on the needs of receiving systems. DPAS has active interfaces with the Unique Item Tracking and Command Asset Visibility and Equipment

Redistribution System. Unique Item Tracking is used to report Army reportable assets to the Continuing Balance System Expanded and to report Small Arms to the Department of Defense Small Arms Serialization Program registry and Cryptology assets to the Controlled Cryptographic Item registry. The Unique Item Tracking interface typically occurs daily with data being sent to Logistics Support Activity when there are Army reportable asset transactions. The Command Asset Visibility and Equipment Redistribution System interface occurs once a week. Both interfaces are controlled by automated system scheduling software.

- *Catalog* - Catalog interfaces are all one-way inbound interfaces. There are active catalog interfaces with Federal Logistics Data, Supply Bulletin 700-20, Army Master Data File, and National Defense Equipment. These interfaces provide DPAS users with current information concerning National Stock Numbers. This information is used by DPAS users to requisition materials and catalog assets. The interface frequencies range from “As Needed” (when updates occur) for the National Defense Equipment, to Semi-Annual for the Supply Bulletin, to monthly for Federal Logistics Data and the Army Master Data File. Defense Logistics Information Service is responsible for sending Federal Logistics Data to DPAS and the Logistics Support Activity is responsible for sending the Supply Bulletin, Army Master Data File and National Defense Equipment data.
- *Excess* - The excess interface is a two-way interface that supports the redistribution of information technology (IT) assets. The interface exchanges asset disposal information with the Defense Reutilization and Marketing Automated Information System. This interface is used to notify managers of excess assets. The Defense Reutilization and Marketing Automated Information System provides DPAS with information about sites that accept excess assets and with information concerning schools that have been approved to participate in the Computers for Learning program.
- *Hand Receipt* - The hand receipt interface is a one-way outbound interface that supports feeding asset information to the ULLS-S4 system. The interface is used to provide DPAS ULLS-S4 users (typically active Army or National Guard units that are stationed at an Army post, camp, or station) information concerning assets acquired by their activity. The data from DPAS is merged with the activity’s own asset data within ULLS-S4 to provide users with a complete picture of assets for which they are responsible. The DPAS user executes this interface in near real-time when there is a need.
- *Maintenance* - The maintenance interface is a one-way outbound interface that supports feeding asset information to external maintenance systems. DPAS has an active maintenance interface with the Facility Equipment

Management System. The interface is used to provide maintenance systems with new equipment receipts, equipment turn-ins, and changes in the status of existing equipment such as serial numbers, bar codes, locations, and accumulated depreciation. The interface provides the maintenance system with approximately 40 attributes on each piece of equipment identified for maintenance and utilization tracking. This interface occurs daily when there is activity and is controlled by automated system scheduling software.

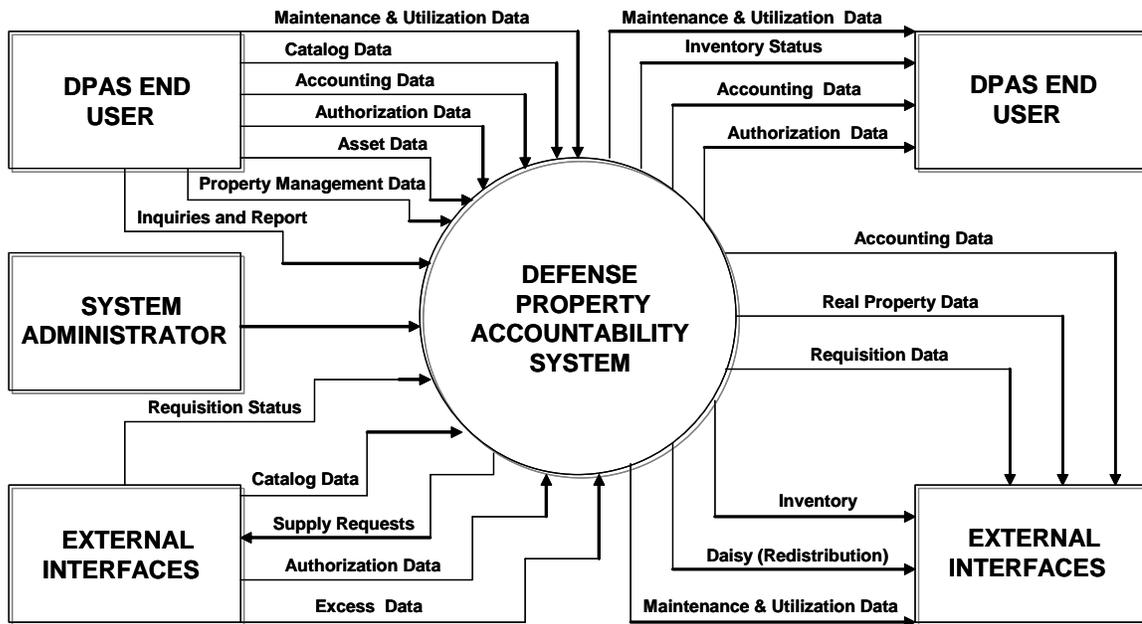
- *Real Property* - The real property interface is a two-way interface. DPAS has active real property interfaces with the Integrated Facilities System and the Planning Resource Infrastructure Decision Evaluation System. The interfaces are used to accept real property information in DPAS. During posting, accounting transactions are generated for transmission to accounting systems. When capital improvements are input directly into DPAS, DPAS generates transactions back to the real property systems to advise them of the improvement. During the DPAS depreciation cycle, DPAS transmits Accumulated Depreciation records to real property systems to update the book value of each asset. This interface typically occurs daily when there is activity and is controlled by automated system scheduling software. The real property systems are responsible for initiating the transmission and receipt of data.
- *Receipts* - The receipts interface is a two-way interface. DPAS has an active receipts interface with the Base Operations Support System. The interface is used to accept information concerning personal property assets posted to users' accounts. Records that reject or are not accepted are sent back to the sending system to advise them that the record was not accepted. This interface typically occurs daily when there is activity and is controlled by automated system scheduling software. Receiving systems are responsible for initiating the transmission and receipt of data.
- *Supply* - Supply interfaces are two-way interfaces that provide users with the ability to perform requisitioning actions using DPAS processes. For the Army Material Command Installation Supply System and the Standard Army Retail Supply System interfaces, these requisitions are transmitted electronically to the Supply Support Activity. The Supply Support Activity issues the material from local stock, or forwards the request to the wholesale level for issuance or to the contracting system for local purchase. In the case of the Defense Automatic Addressing System interface, requisitioning is limited to National Stock Numbers. These requisitions are transmitted directly to the Defense Automatic Addressing System, which in turn retransmits them to the correct Inventory Control Point for issuance. All of the supply systems send requisition status information back to DPAS and DPAS updates the users' requisitions electronically. With the exception of the Defense Automatic Addressing System interface, which is controlled by automated system scheduling

software, these interfaces typically occur daily and are initiated by the user.

Figure 1 below provides a graphical representation of the DPAS data flow.

Figure 1:

DPAS Data Flow



System Architecture

DPAS operates in a client-server environment. This environment provides the application support, operations, backup, and recovery for the DPAS mission. The client environment is comprised of multiple sites employing workstations with connectivity to the server environment. Client connectivity is provided by the server site based on authenticated users with valid internet protocol addresses. DPAS system servers support all DoD agency databases using the DPAS application for property accountability. The server environment consists of the application software, operating system, database, and hardware.

The DPAS database is a relational collection of data associated with property accountability and equipment management. There are 329 relational databases supporting a worldwide geographical dispersion of multiple agencies and

commands. DPAS database files reside on magnetic disk. Magnetic tapes are used for off-line backups of the databases. The storage requirement for each customer database is based primarily on the number of items on the customer's property book. The minimum storage requirement for the DPAS common database is 1.3 Gigabytes. This supports up to 15,000 property book items. Each additional 15,000 property book items increases the storage requirement by 20 Megabytes. The database permits asset authorization, cataloging, accountable record processing, financial processing, equipment maintenance, and equipment utilization. The DPAS Common database is comprised of several individual customer databases and one DPAS Excess database. The physical structure of the DPAS database is such that access to individual databases and the Excess database by the application software is DPAS platform-transparent (the application software is not dependent on the physical location of databases as configured across DPAS platforms). Individual site DPAS databases are resident on the DPAS production servers located at DISA Dayton. The minimum storage requirement for the DPAS Excess database is also 40 Megabytes. In the event of data loss or corruption, the entire DPAS database can be restored from daily tape backups.

The hardware platforms for the DPAS application are Hewlett Packard (HP) L2000, HP K570, HPI70, HPK220, and HPK400 servers. The operating system is a HP-UX Release 11 Operating System with multi-user licensing for concurrent users. Development software includes Micro Focus Version 4.0 COBOL with database environment of Cincom SUPRA 2.9.X Relational Database Management System (UNIX/Client Server version) and Micro Focus Application-to-Application. Servers are remotely managed by system administrators in the DISA Ogden System Management Center (SMC) located at Hill Air Force Base, Ogden, UT.

Security against unauthorized access to the DPAS database is controlled at several levels. End-user access is controlled by the operating system and Remote Defense Business Management System software, as well as by DPAS application software. Database support and maintenance operations can be done only by those individuals designated as database administrators or system administrators.

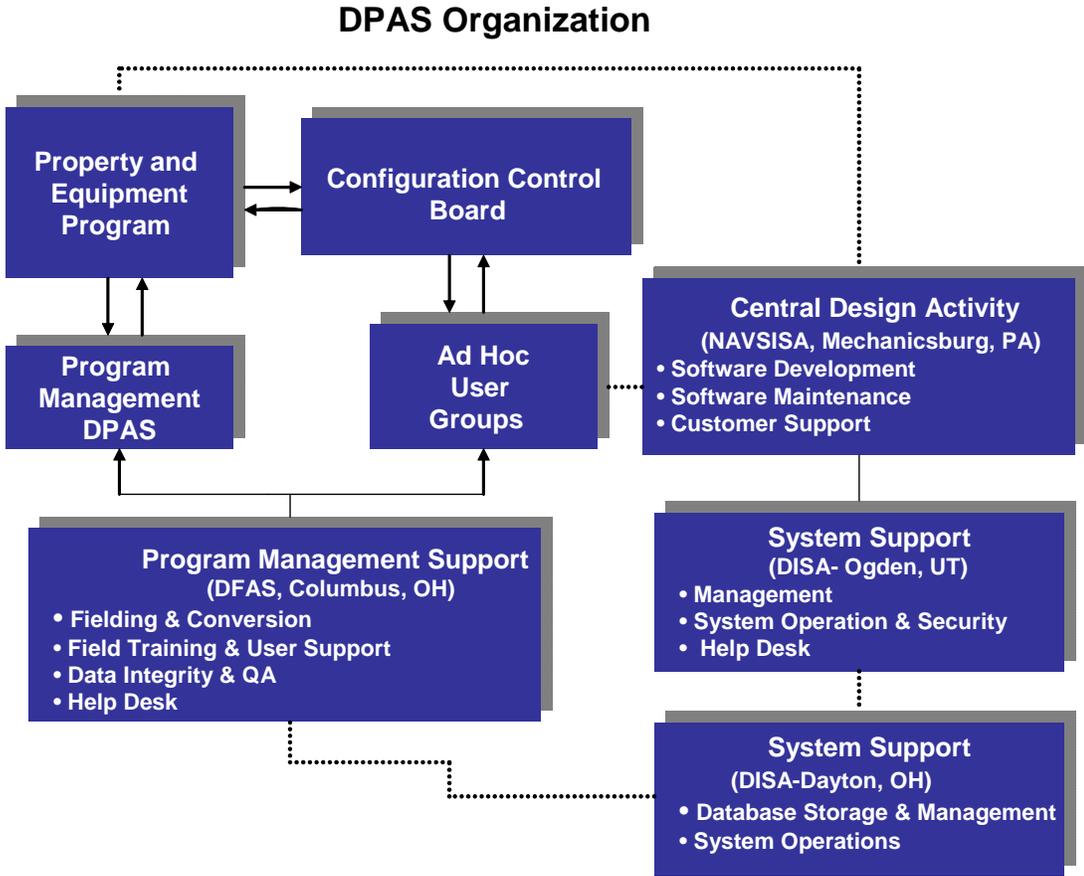
B. Control Environment

Management Oversight

DPAS is a centrally funded and managed program. The Program Manager for DPAS reports to the Deputy Director, Acquisition Resources and Analysis, Property and Equipment Policy Office, which reports to the OUSD(C) and the OUSD, AT&L. The DPAS Program Management Office is located at DFAS, Columbus, Ohio, which provides direct operational oversight for the program and supports all customer service requirements (including data conversions, centralized help desk support, training, quality assurance, site support, e-learning, and website services). DFAS coordinates with DISA SMC Ogden to provide

program IT infrastructure support. Additionally, DFAS and DISA Ogden SMC work closely with NAVSISA for all DPAS software development, maintenance, and testing. Finally, these entities work closely with the DPAS Configuration Control Board (CCB), made up of headquarters level property managers representing the user community, to review the application’s functionality, propose changes, and provide recommendations as needed. The CCB meetings also provide DoD property managers with a forum to learn from each other and share solutions to common problems. Figure 2 below provides a graphical representation of the DPAS oversight and support structure.

Figure 2:



Personnel Policies and Procedures

Hiring practices at each of the service organizations are in accordance with DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003, availability control, “IA Documentation,” which requires that all appointments to required IA roles are established in writing, including assigned duties and appointment criteria such as training, security clearance and IT-designation. DPAS management, support employees, and contractors at DFAS, DISA, and NAVSISA are required to review applicable administrative orders, policies, and procedures with the Human Resource Office and must complete appropriate forms to gain access to the DPAS System. New employees meet with the Information Systems Security Manager to understand their roles and

responsibilities. The Information Systems Security Manager is responsible for: (1) providing basic systems security awareness training (2) securing civilian and contractor signatures on Automated Data Processing Security Awareness disclosure forms, (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 to DPAS when an employee or contractor is hired or terminated.

The mission assurance category (MAC) of an information system reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the war fighter combat mission. MACs are the basis for determining availability and integrity control requirements. In accordance with DoD Directive 8500.1 and DoD Instruction 8500.2, the MAC for DPAS has been determined to be MAC III. MAC III is defined as a system that, "...handles information necessary to conduct day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term." MAC III applications require protective measures, techniques, or procedures generally commensurate with commercial best practices. The confidentiality level of the system has been established as Sensitive. The DPAS System Security Authorization Agreement (SSAA) addresses the requirements for background checks, gaining access to the application, and segregation of duties for support personnel and the user community. This includes controlling access to DPAS by using identification and authentication mechanisms such as User IDs and passwords, and using discretionary access, auditing, and object reuse controls. DPAS operates with the following objectives:

- a. DPAS information shall be handled as sensitive but unclassified.
- b. Adequate measures shall be in effect to ensure that data is being transferred securely across communication channels.
- c. All access through firewalls will be authenticated.
- d. Identification and Authentication will be accomplished within DPAS by using unique user logins and passwords.
- e. Discretionary Access Controls will be implemented within databases.

User Accounts are managed by the System Administrator located at the DISA Ogden SMC and by Site Security Officers. Personnel requesting access to DPAS are required to submit a System Authorization Access Request (SAAR), DD Form 2875, including the status of the user's background check and clearance level to the DISA Ogden Security Office prior to being granted access. Completion of the form requires the user to accept the User Agreement to comply with DISA and DoD security policies and the responsibility for safeguarding information contained in the system. Within their capabilities, each user shall protect information and automated information systems resources against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons. Users shall report all such

occurrences to their TASO or Information Assurance Officer (IAO) immediately.

DPAS developers and maintainers at DFAS, DISA, and NAVSISA, as well as the end users, are required to have favorable personnel background investigations. The level of investigation depends on the sensitivity level of the automated data processing (ADP) position assigned to each individual in accordance with the DoD 5200.2-R, "Personnel Security Program Regulation," issued January 1987, and the DoD 5220.22-M, "National Industrial Security Program Operating Manual," issued January 1995.

Individuals in positions designated ADP-I require a Single Scope Background Investigation. Examples of positions that are designated ADP-I are Designated Approving Authorities (DAA), Program Managers, System Managers, Information System Security Managers, and Network Security Managers. All local area network administrators who have the ability to assign user-IDs and passwords or the capability to grant access to sensitive files will also occupy ADP-I positions. The Director of DFAS may assign ADP-I sensitivity levels to other unique positions.

Individuals in positions designated ADP-II and ADP-III require a National Agency Check Plus Written Inquiries, or an equivalent level of investigation. Persons assigned ADP-II designations do not make executive decisions regarding management of IT systems, hardware, or software, and are subordinate to ADP-I positions. These positions include IAOs, TASOs, application and systems programmers, operators, customer service personnel, schedulers, tape librarians, and secretaries. All other positions involved in DPAS activities should be assigned ADP-III except for contractor positions that require a National Agency Check investigation only.

Training

Personnel at DFAS, DISA, and NAVSISA are required to complete continuing education. Training objectives for continuing education are captured in the Individual Development Plans by each individual and their supervisor.

DPAS training is obtained by service organization personnel through the DPAS Security Awareness Guide, DPAS Operational Support Team Troubleshooting Guide, and Knowledge Management system. The DISA Online Training System provides training-related technical services used in the DPAS application. Support personnel at DFAS, DISA, and NAVSISA are required to receive annual security awareness training through their respective agency or service. Each agency or service is required to follow the DoDI 8500.2 guidelines in providing security awareness training. In addition, DPAS application-specific security training covers roles and responsibilities for the DPAS end user. Documentation of training is recorded in an attendance roster and a certificate of completion is provided to each user. Training is monitored for content and kept up-to-date by

agency or service security and training coordinators. Training for the user community is offered by DFAS but is not required.

Security training focuses on those processes that ensure only authorized users gain access to the application and specific programs. DPAS IAO's and Technical Points of Contact are provided training for proper access control and setting up user profiles at the DPAS program and user levels. This training is provided in conjunction with the standard courses for DPAS Basic and Basic Plus.

The DPAS User Training Manual addresses administrative issues such as granting security access, assigning multiple accountable UICs to users, modifying the DPAS program, and user access. In addition, DPAS users receive the DPAS Security Awareness Guide that explains security awareness and appropriate measures to safeguard the system. The guide is provided to users when new accounts are set up, during training, and annually.

C. Monitoring

Management and supervisory personnel at DFAS, DISA, and NAVSISA monitor the performance quality and internal control environment as a normal part of their activities. DFAS, DISA, and NAVSISA implemented a number of management, quality assurance, and operational reports that help monitor the performance of DPAS processing as well as the DPAS system itself. These reports are reviewed by DFAS, DISA, and NAVSISA. Corrective action is taken as necessary. DPAS processing problems and exceptions to normal or scheduled processing through hardware or software are logged, reported, and resolved.

DISA Field Security Operations

DPAS is subject to a System Readiness Review (SRR) process that consists of running automated SRR scripts and manual checks to compare DPAS system security settings to recommended security settings documented in the DISA Security Technical Implementation Guides (STIGs). These SRRs include only the software portion of the STIG. The SRR process is performed on the DPAS operating system, the database management system, and web services. DISA system administrators are responsible for executing and tracking the SRR processes on a weekly basis. Findings noted during the SRR processes are monitored at DISA, Montgomery, AL. The DISA Field Security Operations (FSO) performs SRRs of systems supported by DISA to determine whether those systems are in compliance with relevant STIGs. The SRR performed by the FSO is a full STIG compliance review that typically occurs annually. The DPAS system components that are maintained by DISA are subject to FSO reviews. The FSO is independent of the DISA Ogden management structure and does not maintain or configure DPAS systems.

Findings noted during the FSO SRR process are categorized according to severity and tracked in the Vulnerability Management System (VMS) database. VMS is

an online web based database with access protected by user IDs and user security profiles. System Administrators, IAOs or Information Assurance Managers (IAM) have the responsibility to close findings in the database as they are mitigated in the systems. A member of the FSO staff must validate finding resolutions. The FSO also performs random validation checks of resolved findings to ensure that corrective actions are actually taking place. Some findings can be exempt from resolution if technical or business needs require a noncompliant setting. Exceptions are usually for a limited time and must be approved by the IAM prior to final approval by the DAA.

The Information Assurance Vulnerability Alert tracking system in the VMS database generates management reports that are checked daily by the IAM to monitor Information Assurance Vulnerability Alert compliance. Results of SA, IAO, and IAM mitigation and closure efforts are provided to the DAA.

DITSCAP Certification and Accreditation

DoD Directive 5200.40, DITSCAP, issued December 30, 1997, and DoD 8510.1-M, "DITSCAP Application Manual," issued July 31, 2000, established the DITSCAP as the standard DoD certification and accreditation process. Certification is the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards made in support of the accreditation process to establish the extent to which a particular design and implementation adheres to specified security requirements. Accreditation is the formal declaration by a DAA 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. DITSCAP establishes a standard process, set of activities, general tasks, and a management structure to certify and accredit an information system that will maintain the IA and security posture of the Defense Information Infrastructure. This process supports an infrastructure-centric approach with a focus on the mission, environment, and architecture.

DPAS must comply with all of the DITSCAP certification and accreditation requirements throughout its life cycle and document the requirements in the SSAA. The SSAA is a formal agreement with the DAA(s), the Certifier, user representative, and program manager employed to guide actions, document decisions, specify IA requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security. SSAAs were prepared for the DPAS application and the supporting operating environment.

Trouble Management System Function

DPAS system problems are usually identified by a DPAS user or by a monitoring process executed at the support organization. The problem is logged into the Trouble Management System maintained by NAVSISA. A trouble ticket number is assigned in the log and a technician to return the system to a fully operational

state is identified and recorded on the ticket. The Trouble Management System is monitored by NAVSISA to ensure tickets are closed timely, and by the Software Director to ensure their knowledge of the operational state of the system. The Trouble Management System ticket is monitored to ensure the completion of the proposed corrective action, as well as actions taken to return the system to full operational capability.

Data Evaluation and Quality Assurance Function

The DFAS Data Evaluation and Quality Assurance function provides recurring and special reports, data extracts, data analysis, and recommendations to improve DPAS data integrity and program efficiency. These reports are generated on a monthly basis, captured electronically onto compact discs, and distributed to CCB representatives. The Quality Assurance branch monitors data quality to measure improvement over time in the areas of asset management, accountability, and financial reporting accuracy.

Department of Defense, Office of Inspector General

The DoD OIG was established by Congress to conduct and supervise audits and investigations related to DoD programs and operations. The DoD OIG reports directly to the Secretary of Defense and is independent of DFAS and DISA. DPAS, as well as the property accountability processes it supports, is part of the DoD OIG audit universe and is subject to financial, operational, and IT audits, reviews, and special assessment projects.

Office of the Inspector General, Defense Information Systems Agency

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 DPAS are part of the DISA Office of the Inspector General audit universe and are subject to audits, inspections, and investigations conducted by the DISA OIG.

D. Risk Assessment

Threats, vulnerabilities, and risks associated with DPAS operations are documented in the application and enclave SSAAs with personnel from DFAS, DISA, and NAVSISA participating in the risk assessments. Among the tools utilized for conducting risk assessments are a comprehensive evaluation of the MAC Controls referenced in DoD Instruction 8500.2 and applicable Phase II, III, and IV tasks documented in DoD 8510.1-M. The MAC controls address the areas of Security Design and Configuration, Identification and Authentication, Enclave and Computing Environment, Enclave Boundary Defense, Physical and Environmental, Personnel, Continuity and Vulnerability, and Incident Management. The procedures outlined in DoD 8510.1-M cover risk in the

following major areas: System Architecture Analysis, Software, Hardware, Firmware Design Analysis, Network Connection Rule Compliance Analysis, Life-cycle Management Analysis, Vulnerability Assessment, Security Testing and Evaluation, Penetration Testing, System Management Analysis, and Contingency Plan Evaluation. The SSAA describes Residual Risk Assessments and documents vulnerabilities noted during DPAS tests and analyses. The SSAA also documents risk mitigation strategies designed to protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification. The SRR processes described in the Monitoring section also provide management a means to assess and track potential security risks associated with the DPAS technical infrastructure.

E. Information and Communication

Users can submit a change request to the DPAS CCB, which makes the final determination on the implementation of changes to the system. There is a documented system request process that considers emerging information needs of the user community.

On an annual basis, each support organization independently develops a DPAS program strategy that is summarized in a support agreement known as a Service-Level Proposal or Service-Level Agreement. The strategies are based on user needs expressed through their CCB member, technology changes, challenges discussed during DPAS program reviews, changes in policies and procedures from the Comptroller and logistics communities, and budgetary realities input from the respective support organizations.

There are three DPAS support agreements in place that are reviewed and updated annually. These Service-Level Agreements detail the roles and responsibilities of the various entities involved in providing support to DPAS.

1. OUSD, AT&L, Arlington, VA, and the Department of the Navy, NAVSISA, Mechanicsburg, PA.

As detailed in the Service-Level Agreement, NAVSISA provides OUSD, AT&L the following services:

- a. Software Development Services
- b. Software Maintenance and Operating Support
- c. Management Reporting
- d. Other Support (Provides briefings to DPAS user groups and user conferences as requested by the customer. Provides software and scanner web-site content as required by the DPAS Web-Site Review Board. Updates DPAS trainer personnel on software changes as required. Provides technical support to various DPAS support initiatives such as e-learning, security documentation, web-site, and

classroom training.)

2. DISA and the OUSD, AT&L.

As detailed in the Service-Level Agreement, DISA provides OUSD, AT&L the following services:

- a. Server Processing
- b. Telecommunications Services
- c. Support Services, including technical and operational support for the DPAS application, Security, System Administration, Network Communications, Database Management, Operations, Customer Technical Liaison, and the Web Server
- d. Full Cost Recovery Services, including processing cycles, input and output transfers, memory utilization, storage of and access to data maintained on direct access storage devices, and network connectivity

3. Director, Property and Equipment Policy, OUSD, AT&L, Arlington, VA, and the Defense Finance Accounting Service Technology Services Organization, DPAS Program Management Support Division.

As detailed in the Service-Level Agreement, DFAS Columbus provides OUSD, AT&L the following services:

- a. Administration
- b. Program planning
- c. Program management support
- d. Customer support that includes implementations, data assurance customer assistance, call center, help desk, web-site development and administration
- e. Customer training
- f. Oversight of the software development and maintenance service provided by NAVSISA, and
- g. Oversight of systems infrastructure support operational services and data processing services provided by DISA

Ongoing written communication between DPAS support community organizations and staff helps to ensure that program objectives and important information are clearly shared. Support organizations also meet to discuss program issues and project objectives including performance, areas of concern, accomplishments, anticipated workload changes, and project status reports. NAVSISA provides weekly status reports on deliverables and services via update of the Configuration Management Tracking System (CMTS). In-Process Reviews are conducted on project status and open management issues. CCB meetings are held biannually to communicate issues including new DPAS

releases to the user community. The DPAS support entities participate with the CCB in meetings, briefings, or site visits to discuss processing and program issues.

The DPAS Help Desk provides customer support from 6 a.m. until 6 p.m. and an on-call service for all other times. The Help Desk mission is to provide customers a single place to call for their support needs. Help Desk agents are responsible for tracking and responding to customer requests including those that come in through the DPAS web site, email, or the Call Center. The agents track issues that require system changes through the Program Trouble Report (PTR) process until they are resolved.

The DPAS program provides a public website that contains information on the DPAS program mission and goals, software, support, training, and guidance. The support areas include customer, technical, security, training, and management support, as well as quality assurance.

F. Control Activities

The DPAS 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 management’s description of controls.

G. User Control Considerations

DPAS was designed with the assumption that certain controls would be implemented by DPAS user organizations. This section describes additional controls that should be in operation at DPAS user organizations to complement the controls maintained by DFAS, DISA, and NAVSISA. User auditors should consider whether the following controls have been placed in operation at user organizations:

Authorization Controls

- Property in transit in which the government has taken title is recorded by the Property Custodian and has been approved by the Property Book Officer (PBO).

- Recorded additions and changes to the asset register and master file made by the Property Custodian are compared to source documents authorized by the PBO to ensure that they were input accurately.
- Assets are periodically inventoried by the Hand Receipt Holder and then the PBO to ensure that hand receipts match assets recorded in the asset register. Reconciling items are identified and addressed by the Hand Receipt Holder in a timely manner.
- Authorized users of DPAS and their specific access needs are approved by the PBO and the Information Systems Security Officer, and directly communicated in writing by the resource owner to DISA-Ogden.
- Personnel responsible for asset acquisition, disposal, recording, and maintenance have responsibility for only one such function and do not have system access to other than their assigned function.
- The Information Systems Security Officer has configured system security so that only authorized users have the ability to enter, modify, or otherwise alter property records.

Completeness Controls

- The PBO and user's accounting function periodically review the asset register and master file data for accuracy, ongoing pertinence, and reconciliation to the corresponding general ledger accounts. Reconciling items are addressed by the PBO in a timely manner.
- The Property Custodian accurately records the values and physical units of beginning balances, acquisitions, and property held for disposal and retirement in DPAS.
- Requests to change the asset register and master file data are logged and reviewed by the PBO to ensure that all requested changes are processed timely.
- Asset-related transactions before or after the end of an accounting period are scrutinized and reconciled by the user's accounting function to ensure complete and consistent recording of transactions in the appropriate accounting period.
- Asset and accumulated depreciation balances are carried forward from one processing cycle to the next by the user's accounting function, using independently obtained asset acquisition, asset disposal, and depreciation expense data.

- Depreciation charges are reviewed by the PBO and the user's accounting function to determine whether the charges are accurate, complete, and recorded in the appropriate period.
- The PBO identifies DoD property accountability policies, communicates those policies to property personnel, and updates standard operating procedures to reflect policy changes.

Accuracy Controls

- The Property Custodian accurately records the method and costs of acquiring each property item or bulk property item.
- Depreciation exception items are consistently identified, monitored, and corrected by the PBO and the user's accounting function.

Control Over The Integrity of Processing and Data Files

- The Property Custodian accurately records property in-transit information to establish and maintain accountability and control over property.
- Processing out-of-balance reports are reviewed promptly by the PBO and the user's accounting function and followed up by the PBO to determine the cause of the out-of-balance condition.
- The PBO periodically reviews error reports that list rejected transactions and corrects them within a reasonable time.
- All changes to the asset register and master file are approved by the PBO.
- The PBO reviews audit trails of changes to property records including a transaction-based history of property activity, modifications, improvements, changes in value, and the data entry and approval.
- Interfaced inputs are transmitted in batch files, and batch control totals are used to balance sent transactions to received transactions. Out-of-balance conditions are reported, corrected, and reentered.

The list of user-organization control considerations presented above does not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations.

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

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

A. Scope Limitations

The control objectives documented in this section were specified by the DoD OIG. The control activities described in this section were specified by DISA, DFAS, and NAVSISA management. As described in the prior section (Section II), DPAS interfaces with many systems. The controls described and tests of these controls in this section of the report were limited to those computer systems, operations, and processes directly related to DPAS itself. The controls related to DPAS source and destination systems interfaces were specifically excluded from this review. We did not perform procedures to evaluate the effectiveness of the input, processing, and output controls within interfacing systems; although we did perform procedures to evaluate DPAS interface input and output controls. We did not perform any procedures to evaluate the integrity and accuracy of the data contained in DPAS.

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

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
<i>Enterprise-Wide Security Program Planning</i>				
1	Risks are periodically assessed.	<p><u>DISA-Ogden, DFAS-Columbus</u> Risk assessments are performed as part of the DITSCAP compliance process. Automated System Readiness Reports (SRR) scripts are run on each server and reported to the Montgomery SRR database on a weekly basis. Each system has an SRR and an Internet Security Systems (ISS) scan performed before it is connected to the network. The DISA FSO runs periodic SRRs and ISS scans. SRR findings are documented and tracked in the VMS.</p>	<p><u>DFAS-Columbus</u> Read the latest Risk Assessment performed with the SSAA and confirmed with the Branch Chief, Quality Assurance Division that risks were periodically assessed.</p> <p>Read the annual IA assessment and confirmed with the ISSO that existing policies and processes were assessed annually.</p> <p><u>DISA-Ogden</u> Observed the SRR process to confirm that it occurred and that corrective actions were tracked.</p> <p>Selected a haphazard sample of SRRs performed by DISA-Ogden and inspected the VMS reports to confirm findings identified by the SRR process had been addressed.</p>	<p>The DITSCAP Phase II and Phase III Summary Analysis Reports for each task were not documented and included in the SSAA. However, a checklist was completed for each Phase II and Phase III task and a Risk Assessment and an IA assessment were performed. The intent of the objective was achieved.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
2	A security plan is documented and approved.	<u>DFAS-Columbus</u> The DPAS security plan is documented, maintained, approved, and periodically updated.	<u>DFAS-Columbus</u> Read the DPAS SSAA to confirm it had been documented, updated and appropriately approved. Read the annual IA assessment to confirm that existing policies and processes were assessed annually.	No relevant exceptions noted.
3	The security plan is kept current.	<u>DFAS-Columbus</u> The DPAS security plan is documented, maintained, approved, and periodically updated.	<u>DFAS-Columbus</u> Read the DPAS SSAA to confirm it had been documented, updated and appropriately approved. Read the DPAS Systems Security Policy, Security Requirements, and Certification Test and Evaluation Plan and Procedures to confirm that each had been updated. Read the annual IA assessment to confirm that existing policies and processes were assessed annually.	No relevant exceptions noted.
4	A security management structure has been established.	<u>DISA-Ogden</u> An IAM and Alternate IAM have been assigned.	<u>DISA-Ogden</u> Confirmed through inquiry that a management structure had been	The security management structure contained position titles

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		There are Information Assurance Officers (IAOs) for each type of operating system and TASOs assigned to each area.	<p>established.</p> <p>Read the DISA-Ogden organizational chart and job descriptions to confirm that all positions were established in writing.</p> <p>Read the SSAA for the security management structure. Confirmed each position was outlined in the SSAA.</p>	that were not in accordance with DOD 8500.2 requirements. However, we confirmed through interviews and inspection of the organizational chart and job descriptions that a security management structure was in place. The intent of the objective was achieved.
5	Information security responsibilities are clearly assigned.	<u>DISA-Ogden</u> An IAM and Alternate IAM have been assigned. There are IAOs for each type of operating system and TASOs assigned to each area.	<p><u>DISA-Ogden</u> Read the SSAA for the security management responsibilities. Confirmed each position outlined in the SSAA was filled and the person understood their duty.</p> <p>Read the DISA-Ogden organizational chart and job descriptions to confirm that all positions were established in writing.</p>	No relevant exceptions noted.
6	A set of rules that	<u>DISA-Ogden</u>	<u>DISA-Ogden</u>	No relevant exceptions

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place.	The DPAS SSAA describes IA responsibilities and expected behavior of personnel.	<p>Obtained the DISA-Ogden SSAA and job descriptions. Confirmed that the SSAA and job descriptions clearly delineated responsibilities and expected behavior.</p> <p>Read the DISA-Ogden organizational chart and job descriptions to confirm that all positions were established in writing.</p>	noted.
7	Owners and users are aware of security policies.	<p><u>DISA-Ogden</u> Each new employee and contactor is provided with a security briefing. They must also sign that they have received this briefing. This briefing is provided annually to employees and contractors.</p>	<p><u>DISA-Ogden</u> Read the Security Awareness Training provided by DISA-Ogden. Selected a haphazard sample of employees and read their training files to confirm the completion of the necessary security training and a signoff.</p> <p>Inspected the training sign-in sheets to confirm that DISA-Ogden employees had attended annual training.</p>	The DPAS Program Manager, DISA- Ogden, did not attend the 2004 annual training. However, the DPAS Program Manager did not have system access to DPAS. As such, the DPAS Program Manager's lack of training presents minimal risk to DPAS.
8	An incident response capability has been	<p><u>DISA-Ogden</u> An incident response</p>	<p><u>DISA-Ogden</u> Confirmed through inspection that</p>	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	implemented.	plan has been established and documented in the DISA-Ogden SSAA.	the incident plan detailed in the SSAA had been implemented. Selected a haphazard sample of incidents to confirm that the incident response plan was being followed.	
9	Hiring, transfer, termination, and performance policies address security.	<p><u>DISA-Ogden</u> For security purposes, all newly hired personnel are required to have:</p> <ol style="list-style-type: none"> 1. Completed National Agency Check personal security investigations for all functional users (civilian, military, and contractors), as a minimum. 2. Registration of all users by Defense Enterprise Computing Center (DECC) System Administrators, IAO, or the specific data owners. 3. Specified system 	<p><u>DISA-Ogden</u> Read the hiring, transfer, termination and performance policies of DISA-Ogden to confirm they were documented.</p> <p>Inspected a haphazard sample of System Access Authorization Request (SAAR) Form 2875 to confirm that each Form 2875 detailed the user's justification for access, security clearance level, and that each Form 2875 was properly approved.</p> <p>Confirmed through inquiry that a debrief is conducted when an employee is terminated and that a DISA Form 70 is used to note the collection of DISA property.</p>	<p>The DPAS Program Manager, DISA- Ogden, did not attend the 2004 annual training.</p> <p>However, the DPAS Program Manager did not have system access to DPAS. As such, the DPAS Program Manager's lack of training presents minimal risk to DPAS.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>and/or application permissions that only allow access to required, ‘need to know’ information.</p> <ol style="list-style-type: none"> 4. Unique User Identification (ID) and password for all users. 5. Specific DECC system training. 6. Initial and refresher Information Security training. 7. DISA Form 2875 for all DECC system users. <p>For transfer and termination of personnel, the following is required:</p> <ol style="list-style-type: none"> 1. Debriefing is conducted. 2. Reminder of the non-disclosure agreement. 3. DISA form 70 checklist is used to ensure collection of 	<p>Confirmed through observation that an email is sent to the Security Administrator to request that system access be removed for a terminated employee.</p> <p>Selected a sample of all DPAS related employees located at DISA-Ogden and inspected the annual security sign-in sheets to confirm that each employee had completed the training.</p>	

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>DISA property.</p> <p>4. Signed DISA termination statement.</p> <p>5. Email is sent to System Administrators to remove all system access.</p>		
10	<p>Employees have adequate training and expertise.</p>	<p><u>DISA-Ogden</u> Employees are required to complete periodic training for their respective job functions.</p>	<p><u>DISA-Ogden</u> Confirmed through inquiry that employees had adequate training and expertise.</p> <p>Read System Administrator training materials to confirm that they provided each System Administrator with adequate training and expertise.</p>	<p>The System Administrator-specific training was outdated and did not provide a means to verify whether a user had successfully completed the training materials. However, we confirmed through inspection of annual security training attendance sheets that DISA-Ogden employees attended annual security training. The intent of the objective was achieved.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
11	<p>A program is implemented to confirm that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities.</p>	<p><u>DISA-Ogden</u> Each new employee and contactor is provided with a security briefing. They must also sign that they have received this briefing. This briefing is provided annually to employees and contractors.</p>	<p><u>DISA-Ogden</u> Read the Security Awareness Training provided by DISA-Ogden. Selected a haphazard sample of employees and read their training files to confirm the completion of the necessary security training and a signoff.</p>	<p>The DPAS Program Manager, DISA- Ogden, did not attend the 2004 annual training. However, the DPAS Program Manager did not have system access to DPAS. The DPAS Program Manager’s lack of training presents minimal risk to DPAS.</p>
12	<p>Management periodically assesses the appropriateness of security policies and compliance with them.</p>	<p><u>DISA-Ogden, DFAS-Columbus</u> An IA review is conducted by the Security Officer that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations.</p>	<p><u>DISA-Ogden</u> Interviewed the Security Officer to obtain an understanding of how DISA-Ogden management assessed the appropriateness of the security policies and compliance with them. Read the DPAS Security Requirements and Information Systems Security Policy Certification Test and Evaluation Procedures to confirm that an annual IA review was conducted and that comprehensive vulnerability management was in place.</p>	<p>The DPAS SSAA was approved by the DAA, on October 9, 2003 providing DPAS with an ATO; however, we determined that the SSAA was not in total compliance with DITSCAP. Since the ATO, We noted that sections of the DPAS SSAA had been updated in accordance to DoDI 8500.2 DCAR-1; however, all required DITSCAP Phase II and</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p><u>DFAS-Columbus</u> Read the annual IA assessment to confirm that existing policies and processes were assessed annually.</p> <p>Read the DPAS SSAA to confirm that the latest risk assessment was conducted in 2003.</p>	<p>III analysis had not been properly performed and documented. We noted, however, that a checklist had been documented for each Phase II and Phase III task.</p>
13	<p>Management ensures that corrective actions are effectively implemented.</p>	<p><u>DISA-Ogden</u> Corrective actions are tested after they have been implemented and monitored on a continuing basis.</p>	<p><u>DISA-Ogden</u> Interviewed management personnel to gain an understanding of how operating system patches, updates and changes were implemented.</p> <p>Observed the SRR process to confirm that corrective actions were implemented for identified SRR findings.</p> <p>Selected a haphazard sample of SRRs and inspected the VMS reports to confirm findings identified by the SRR process had</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
14	<p>A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place.</p>	<p><u>DISA-Ogden</u> Software and hardware vulnerabilities are independently validated through inspection and automated vulnerability assessment or state management tools. VMS and Information Assurance Vulnerability Alert are utilized to track and maintain system vulnerability status.</p>	<p>been addressed. <u>DISA-Ogden</u> Read the vulnerability management policy to confirm that the process included systematic identification and migration of software and hardware vulnerabilities had been documented and resolved.</p>	<p>No relevant exceptions noted.</p>
15	<p>Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.</p>	<p><u>DISA-Ogden</u> SRR scripts are run on each server and reported to the Montgomery SRR database on a weekly basis. Each system has an SRR and an ISS scan performed before it is connected to the network. The DISA FSO runs periodic SRRs and ISS scans. All system</p>	<p><u>DISA-Ogden</u> Observed the SRR process to confirm that it occurred and that corrective actions were tracked.</p> <p>Observed the system software change control process for DISA-Ogden and confirmed that changes were properly approved before implementation.</p> <p>Inspected a sample of system changes and confirmed that</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		software changes must be reviewed and approved prior to implementation.	changed were only implemented after proper approval or not implemented if not approved.	
16	A DoD reference document constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products.	<u>DISA-Ogden</u> The DISA UNIX STIG, and DISA Instruction Information Systems Security Program 630-230-19 are the primary documents used to frame the internal security requirements of the DPAS application.	<u>DISA-Ogden</u> Read the DoD Directives 8500.01, 8500.02, 8510.1-M, the DISA Database STIG, DISA UNIX STIG, and DISA Instruction Information Systems Security Program 630-230-19 to confirm that they constituted the primary source configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled products.	No relevant exceptions noted.
	<i>Access Controls</i>			
17	Resource classifications and related criteria have been established.	<u>DFAS-Columbus</u> The MAC Level has been assigned and periodically reviewed.	<u>DFAS-Columbus</u> Read the DPAS SSAA and confirmed that a MAC level had been assigned to DPAS and reviewed.	No relevant exceptions noted.
18	Owners have classified resources.	<u>DFAS-Columbus</u> The MAC Level has been assigned and periodically reviewed.	<u>DFAS-Columbus</u> Read the DPAS SSAA and confirmed that a MAC level had been assigned to DPAS and reviewed.	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
19	Resource owners have identified authorized users and their level of access.	<u>DFAS-Columbus</u> User access roles within DPAS are defined according to job description, Modules Accessed, Access Privilege, Required Module, Module Sensitivity, and Position Sensitivity.	<u>DFAS-Columbus</u> Observed documentation that defined user roles and responsibilities. Observed the application to confirm that users required a valid Login and Password to gain access to the system. Observed that a user account was assigned a Security Profile that restricted access by module, program, Unit Identification Code (UIC), and Hand Receipt.	No relevant exceptions noted.
20	Emergency and temporary access authorization is controlled.	<u>DISA-Ogden</u> Emergency and temporary access authorizations are documented on standard forms and maintained on file, approved by appropriate managers, securely communicated to the security function, and automatically terminated after a	<u>DISA-Ogden</u> Read the emergency and temporary access policy. Selected a sample of emergency and temporary access and confirmed that: <ul style="list-style-type: none"> • The authorization was approved and that access was closed in a timely manner. • The emergency and temporary access list was periodically reviewed. 	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		predetermined period.	<ul style="list-style-type: none"> • Temporary access authorizations were established for least privileged need-to-know access. 	
21	Owners determine disposition and sharing of data.	<p><u>DISA-Dayton</u> The “Disposition of Unclassified DoD Computer Hard Drives” policy is followed for the disposal of equipment containing sensitive information and software.</p> <p><u>DFAS-Columbus</u> Security Profiles in DPAS limit the DPAS Modules that can be accessed by a user and the functionality provided within those DPAS Modules.</p>	<p><u>DISA-Dayton</u> Obtained and read the “Disposition of Unclassified DoD Computer Hard Drives” policy used by DISA-Dayton. Conducted inquiry of DPAS Database Administrator and confirmed that the policy was being used.</p> <p>Observed the destroyed hard drives located at DISA-Dayton.</p> <p><u>DFAS-Columbus</u> Observed that each user account was assigned a Security Profile that restricted access by module, program, UIC, and Hand Receipt.</p>	No relevant exceptions noted.
22	Adequate physical security controls have been implemented.	<u>DISA-Ogden, DISA-Dayton</u> Physical and logical access controls are in	<u>DISA-Ogden</u> Observed the physical safeguards in place for DISA Ogden to confirm safeguards had been established to	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>place to restrict employees to authorized actions based on organizational and individual job responsibilities.</p> <p>Every physical access point that displays sensitive information or unclassified information that has not been cleared for release is controlled during business hours and guarded or locked during non-business hours. Current signed procedures exist for controlling visitor access.</p>	<p>mitigate the risk of physical damage or access.</p> <p>Observed that facility penetration testing processes were in place that included periodic, unannounced attempts to penetrate key computing facilities and that every physical access point that displayed sensitive information or unclassified information that had not been cleared for release was controlled during business hours and guarded or locked during non-business hours.</p> <p><u>DISA-Dayton</u> Confirmed through observation that physical safeguards had been established at DISA-Dayton to mitigate the risk of physical damage or access.</p> <p>Observed that facility penetration testing processes were in place that included periodic, unannounced</p>	

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>attempts to penetrate key computing facilities and that every physical access point that displayed sensitive information or unclassified information that had not been cleared for release was controlled during business hours and guarded or locked during non-business hours.</p>	
23	<p>Physical safeguards have been established that are commensurate with the risks of physical damage or access.</p>	<p><u>DISA-Dayton</u> All packages entering into DISA-Dayton are inspected by entry control for possible bombs. Panic buttons notify Security in the case of an emergency. The notified Security Forces immediately notify all posts and patrols and furnish them with all available information. Security forces seal off the immediate area of DECC-Dayton, or installation</p>	<p><u>DISA-Dayton</u> Confirmed through inspection of penetration exercise documentation that facility penetration testing processes were in place that included periodic, unannounced attempts to penetrate key computing facilities and that every physical access point that displayed sensitive information or unclassified information that had not been cleared for release was controlled during business hours and guarded or locked during non-business hours.</p> <p>Observed that the DPAS data</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>entry exit points may be blocked.</p> <p>Fire suppression and prevention devices are installed in the DPAS data center.</p> <p>Visitors must sign-in with the DISA-Dayton Security Attendant prior to entry into the DISA-Dayton facility.</p>	<p>center was protected by fire suppression and the prevention devices were installed and working. Observed that there was a UPS and that the cooling system was periodically maintained.</p> <p>Confirmed through observation that DISA Dayton contained a master power switch to stop power to IT equipment was in place and was located at the data center entrances and was clearly labeled.</p>	
24	Visitors are controlled.	<p><u>DISA-Ogden, DISA-Dayton</u></p> <p>Entry control is manned during normal business hours, 0700-1600, Monday – Friday. The entry control personnel manage and maintain the entry point, check badges, and issue visitor</p>	<p><u>DISA-Ogden</u></p> <p>Read the visitor policy and procedure for DISA-Ogden to confirm they were documented. Observed the visitor check in and check out process for DISA-Ogden.</p> <p>Confirmed through inquiry and observation that visitor access to DoD information was determined</p>	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		badges.	<p>by both</p> <p>its classification and user need-to-know.</p> <p><u>DISA-Dayton</u> Confirmed through inquiry that all visitors were controlled.</p> <p>Read the DOD OI 125-5 to confirm that the instruction detailed the procedures for obtaining access and detailed the security procedures for access to controlled areas.</p> <p>Read the Department of the Air Force’s penetration memorandum to confirm that a penetration exercise was preformed by the SFS on the DISA-Dayton facility.</p>	
25	Adequate logical access controls have been implemented at the application layer.	<u>DISA-Ogden</u> A SAAR form is required to be completed and authorized before a user is issued access to the application layer of the system.	<u>DISA-Ogden</u> Inspected a haphazard sample of SAAR Form 2875 to confirm that each Form 2875 detailed the user’s justification for access, security clearance level, and that each Form 2875 was properly approved.	We noted that 4 out of 45 users tested did not have a System Access Authorization Request form on file. According to DISA-Ogden personnel, the missing forms resulted

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Columbus</u> Security Profiles in DPAS limit the DPAS Modules that can be accessed by a user and the functionality provided within those DPAS Modules.</p>	<p><u>DFAS-Columbus</u> Observed that each user account was assigned a Security Profile that restricted access by module, program, UIC, and Hand Receipt.</p>	<p>from the transfer of responsibility for the forms from DISA-Dayton to DISA-Ogden. DISA-Ogden believed they were lost during the physical transfer of the forms from DISA-Dayton to DISA-Ogden. The DISA-Ogden Contract Technical Requirement Analyst indicated to us that these four users were authorized to have access to the system based on daily interaction processing authorization requests. Confirmed through inquiry of the IT Specialist, User Creation Division, and observed a sample of user access forms to that DPAS user accounts and necessary documentation was on file.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
26	<p>Passwords, tokens, or other devices are used to identify and authenticate users.</p>	<p><u>DISA-Ogden, DFAS-Columbus</u> Passwords are used to identify and authenticate users when accessing the DPAS application.</p>	<p><u>DISA-Ogden</u> Confirmed through inquiry that passwords were used to authenticate users.</p> <p>Read the Security Account Creation Guide at DISA-Ogden to confirm that authentication devices were in compliance with DoD standards.</p> <p><u>DFAS-Columbus</u> Observed the DPAS application to confirm that users needed a valid User ID and Password to gain access to the system.</p> <p>Observed that accounts became locked after three failed login attempts.</p>	<p>No relevant exceptions noted.</p>
27	<p>Access paths are identified as part of a risk analysis and documented in an access path diagram.</p>	<p><u>DISA- Oklahoma City (OKC)</u> Access control lists (ACL) have been implemented for interconnections among DoD information systems. The ACLs are controlled by DISA-</p>	<p><u>DISA-OKC</u> Confirmed through inquiry that ACLs, user management controls, firewalls, intrusion detection systems (IDS), and authentications were all used to control network access.</p> <p>Observed the existence of the ACLs</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		OKC.	<p>at DISA-Dayton by having a network administrator display the listing on his desktop.</p> <p>Obtained and read the network diagrams for DISA-Ogden and DISA-Dayton to confirm that access paths were documented and monitored by IDSs.</p>	
28	Access is restricted to data files and software programs.	<p><u>DISA-Ogden, DISA-Dayton</u> Access to data files and software programs is limited to authorized personnel on a “need-to-know” basis.</p>	<p><u>DISA-Ogden, DISA-Dayton</u> For the DPAS servers, confirmed through inquiry and inspection of root access users that access restrictions had been established around the data files and software programs.</p> <p>Inspected the access logs and corroborated with management that the access logs were reviewed for inappropriate access and that system libraries were managed and maintained to protect privileged programs.</p>	No relevant exceptions noted.
29	Access settings have been implemented in	<u>DISA-Ogden, DFAS-Columbus</u>	<u>DISA-Ogden</u> Inspected a haphazard sample of	We noted that 4 out of 45 users tested did not have

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	<p>accordance with the access authorizations established by the resource owners.</p>	<p>Access to data files and software programs is limited to authorized personnel on a “need-to-know” basis.</p>	<p>SAAR Form 2875 to confirm that each Form 2875 detailed the user’s justification for access, security clearance level, and that each Form 2875 was properly approved.</p> <p><u>DFAS-Columbus</u> Observed the DPAS system to confirm that each user account was assigned a Security Profile that restricted access by module, program, UIC, and Hand Receipt.</p>	<p>a System Access Authorization Request form on file. According to DISA-Ogden personnel, the missing forms resulted from the transfer of responsibility for the forms from DISA-Dayton to DISA-Ogden. DISA-Ogden believed they were lost during the physical transfer of the forms from DISA-Dayton to DISA-Ogden. The DISA-Ogden Contract Technical Requirement Analyst indicated to us that these four users were authorized to have access to the system based on daily interaction processing authorization requests. Confirmed through inquiry of the IT Specialist, User Creation Division, and observed a</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				sample of user access forms to that DPAS user accounts and necessary documentation was on file.
30	Telecommunications controls are properly implemented in accordance with authorizations that have been granted.	<p><u>DISA-OKC</u> The following are used to provide telecommunication controls:</p> <ul style="list-style-type: none"> • ACLs, • IDS, • Firewalls, • Encryption, and • Network monitoring. 	<p><u>DISA-OKC</u> Confirmed through inquiry that telecommunications controls were implemented.</p> <p>Observed the existence of ACL, IDS, Firewalls, Encryption, and Network monitoring controls.</p> <p>Using an automated tool, performed passive network monitoring of DPAS related network traffic over a period of 10 days to test for unauthorized network connections.</p>	No relevant exceptions noted.
31	Procedures are in place to clear sensitive information and software from computers, disks, and other equipment or media when they are disposed of or	<p><u>DISA-Dayton</u> The “Disposition of Unclassified DoD Computer Hard Drives” policy is followed for the disposal of equipment containing sensitive information and</p>	<p><u>DISA-Dayton</u> Read the “Disposition of Unclassified DoD Computer Hard Drives” policy used by DISA-Dayton.</p> <p>We confirmed policy was being used through the DPAS Database</p>	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	transferred to another use.	software.	Administrator. Observed the destroyed hard drives located at DISA-Dayton.	
32	Audit trails are maintained at the application layer, operating system, and database layer.	<u>DISA-Ogden, DISA-Dayton</u> Operating System and database audit files are periodically moved to an audit server located at Ogden. The audit files are then transferred to CD and stored on site for one year. After one year, the CDs are destroyed. <u>DFAS-Columbus</u> The DPAS application maintains a History Inquiry of each asset that allows a user to view an audit trail of transactions for an asset.	<u>DISA-Ogden, DISA-Dayton</u> Confirmed through inquiry that DISA-Ogden, DISA-Dayton, and DFAS-Columbus had implemented audit trails at the application layer, operating system, and database layer. Confirmed through inquiry of the Assistant ISSO that audit trails were maintained and logs were read. Confirmed through inquiry of the DPAS DBA and SA that DISA-Ogden personnel routinely reviewed the logs. Confirmed through inquiry and observation that audit logs included activities that might modify, bypass, or negate safeguards controlled by the system and the Audit trails were stored on CDs in the DISA-Ogden facility and protected against unauthorized access, modification, or deletion and were maintained for	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>1 year and then destroyed.</p> <p><u>DFAS-Columbus</u> Observed that the DPAS History Inquiry captured transactional activity of asset.</p>	
33	<p>The contents of audit trails are protected against unauthorized access, modification or deletion.</p>	<p><u>DISA-Ogden, DISA-Dayton</u> Only the IAM, the Assistant IAM, Database Administrator and the HP/UX System Administrators had access to the audit trails.</p>	<p><u>DISA-Ogden, DISA-Dayton</u> Read the policy and procedures for protection of the audit trails and noted that policy limiting access to these audit trails was documented.</p> <p>Observed that only the IAM, the Assistant IAM, Database Administrator and the HP/UX Systems Administrators had access to the audit trails. Attempted to access the audit trails using a test account.</p>	<p>No relevant exceptions noted.</p>
34	<p>Tools are available for the review of audit records and for report generation from audit records.</p>	<p><u>DISA-Ogden, DISA-Dayton</u> The Hewlett Packard Audit Trail tools can be used to review and</p>	<p><u>DISA-Ogden, DISA-Dayton</u> Confirmed through inquiry of DISA-Ogden personnel that a tool was not available to efficiently review audit records.</p>	<p>DISA-Ogden did not have a software tool available to proactively monitor or review operating system audit</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>report existing audit records.</p>		<p>trails because they did not have the appropriate software tool that would allow them to efficiently analyze large volumes of audit log data.</p>
<p>35</p>	<p>Actual or attempted unauthorized, unusual, or sensitive network access is monitored.</p>	<p><u>DISA-Ogden, DISA-OKC</u> Authorized and unauthorized network access is monitored through Transmission Control Protocol (TCP) Wrapper and Klaxon or Banshee. Host based IDS (Symantec Enterprise Security Manager (ESM) and Intruder Alert) are installed on all Unix servers.</p>	<p><u>DISA-Ogden, DISA-OKC</u> Inquired with the System Administrator to confirm that unauthorized, unusual, or sensitive access was monitored.</p> <p>Confirmed through inquiry and observation that DISA currently had network, firewall, and IDS logs. These logs were monitored and maintained to include full audit trails including syslogs and were retained indefinitely.</p> <p>Confirmed through inquiry and observation that authorized and unauthorized network access authorizations were appropriately limited by user management, ACLs, Firewalls, authentication, and network monitoring.</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
36	Suspicious or irregular access activity is investigated and appropriate action taken.	<u>DISA-Ogden</u> When suspicious activity is detected, an initial investigation is performed. If deemed an actual event, the Continental U.S. (CONUS) Regional Computer Emergency Response Team's (RCERT) is notified and action is taken as required.	<u>DISA-Ogden</u> Inquired with System Administrator to confirm that suspicious or irregular access activity was investigated and appropriate actions were taken. Obtained and read evidence that the investigations and corrective actions had taken place.	No relevant exceptions noted.
37	The acquisition, development, and/or use of mobile code to be deployed in DoD systems meet current guidelines, standards and regulations.	<u>DISA-Ogden</u> No mobile code is used on the DPAS servers. <u>DISA Oklahoma City (DISA-OKC)</u> All IA devices have been approved by NSA or in accordance with NSA before acquiring and implementing.	<u>DISA-Ogden</u> Inspected the DoD systems guidelines, standards, and regulations concerning mobile codes. Inquired with the System Administrator to confirm that the acquisition, development, and use of mobile code to be deployed in DoD systems met current guidelines,	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>standards and regulations.</p> <p><u>DISA-OKC</u> Confirmed through inquiry that DISA-OKC verified NSA evaluation or evaluation in accordance with NSA approval for all IA related products.</p> <p>Read the National Information Assurance Partnership (NIAP) website and confirmed that the website provided a list of approved products that included the products being used by DPAS.</p>	
38	<p>All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates.</p>	<p><u>DISA-Ogden, DISA-Dayton</u> All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates.</p>	<p><u>DISA-Ogden, DISA-Dayton</u> Observed that all servers, workstations and mobile computing devices implemented virus protection that included a capability for automatic updates for all DPAS locations.</p> <p>Obtained print screen as evidence that virus protection settings had been configured.</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
39	All Virtual Private Network (VPN) traffic is visible to network IDS.	<u>DISA-OKC</u> All network traffic, including VPN traffic is visible to the RealSecure IDS.	<u>DISA-OKC</u> Inquired with System Administrators to confirm that all VPN traffic was visible to network IDS. Read system network diagram and corroborated with the SA to confirm that VPN traffic was included on the diagram.	No relevant exceptions noted.
40	At a minimum, medium-robustness Commercial Off-the-Shelf IA and IA-enabled products are used to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system.	<u>DISA-OKC</u> All networks managed by DISA-OKC have been encrypted in accordance with the National Institute of Standard and Technology (NIST) cryptography standards.	<u>DISA-OKC</u> Inquired with Key Personnel to confirm that medium-robustness Commercial off-the-Shelf IA and IA-enabled products were used to protect sensitive information when the information transited public networks or the system handling the information was accessible by individuals who were not authorized to access the information on the system for each of the DPAS locations. Using an automated tool, performed passive network monitoring of DPAS related network traffic over a period of 10	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>days to test for unencrypted traffic transmitted over commercial or wireless networks.</p>	
<p>41</p>	<p>Unless there is an overriding technical or operational problem, workstation screen-lock functionality is associated with each workstation.</p>	<p><u>DISA-Ogden</u> Unless there is an overriding technical or operational problem, workstation screen-lock functionality is associated with each workstation. When activated, the screen-lock function places an unclassified pattern onto the entire screen of the workstation, totally hiding what was previously visible on the screen.</p>	<p><u>DISA-Ogden</u> Confirmed through observation that workstation screen-lock functionality was applied. If screen-locks were not being used, confirmed through inquiry the reason with the DPAS SA.</p>	<p>No relevant exceptions noted.</p>
<p>42</p>	<p>Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a</p>	<p><u>DISA-OKC</u> Instant messaging is prohibited at all DISA sites.</p>	<p><u>DISA-OKC</u> Inquired with DISA-Ogden Staff to confirm that no instant messaging was used.</p> <p>Using an automated tool,</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	public service provider is prohibited within DoD information systems.		performed passive network monitoring of DPAS related network traffic over a period of 10 days to test for instant messaging traffic.	
43	For Automated Information System applications, a list of all (potential) hosting enclaves is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements.	<u>DISA-Ogden</u> The DPAS hosting enclaves are documented in the DPAS SSAA.	<u>DISA-Ogden</u> Read the DPAS SSAA to confirm the DPAS enclave and backup enclave had been identified and documented.	No relevant exceptions noted.
44	Group authenticators for application or network access may be used only in conjunction with an individual authenticator.	<u>DISA-Ogden</u> A SAAR Form 2875 is sent to Ogden to request access to DPAS. Ogden then verifies required field contents and signatures. Ogden creates User IDs and passwords and retains the Form 2875. User location's DPAS Security Officer applies the user	<u>DISA-Ogden</u> Confirmed through inquiry if group authenticators for application or network access were used only in conjunction with an individual authenticator. Confirmed through inquiry that if used in conjunction with individual authenticators approval had been given by the DAA.	We noted that 4 out of 45 users tested did not have a System Access Authorization Request form on file. According to DISA-Ogden personnel, the missing forms resulted from the transfer of responsibility for the forms from DISA-Dayton to DISA-Ogden.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>access permissions.</p> <p><u>DFAS-Columbus</u> Users must possess a valid User ID and password to gain access to DPAS.</p>	<p>Inspected a haphazard sample of SAAR Form 2875 to confirm that each Form 2875 detailed the user's justification for access, security clearance level, and that each Form 2875 was properly approved.</p> <p><u>DFAS-Columbus</u> Observed DPAS to confirm that users must possess a valid Login and Password to gain access to the system. Observed the entering of an invalid User ID and password to confirm that the system displayed an error message to the user.</p>	<p>DISA-Ogden believed they were lost during the physical transfer of the forms from DISA-Dayton to DISA-Ogden. The DISA-Ogden Contract Technical Requirement Analyst indicated to us that these four users were authorized to have access to the system based on daily interaction processing authorization requests. Confirmed through inquiry of the IT Specialist, User Creation Division, and observed a sample of user access forms to that DPAS user accounts and necessary documentation was on file.</p>
45	To help prevent inadvertent disclosure of	<p><u>DISA-Ogden</u> All contractors are</p>	<p><u>DISA-Ogden</u> Obtained a listing of all contractor</p>	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	<p>controlled information, all contractors and foreign nationals are identified by e-mail addresses and display names.</p>	<p>identified by the inclusion of the abbreviation “ctr” and all foreign nationals are identified by the inclusion of their two character country code.</p>	<p>and foreign national email addresses and display names for DISA Ogden and confirmed that their proper identifications were present.</p>	
<p>46</p>	<p>Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography.</p>	<p><u>DISA-OKC</u> All networks managed by DISA-OKC have been encrypted in accordance with NIST cryptography standards.</p>	<p><u>DISA-OKC</u> Inquired with Key Personnel to confirm that NIST cryptography was used to protect information when the information transited public networks or the system handling the information was accessible by individuals who were not authorized to access the information on the system for each of the DPAS locations.</p> <p>Using an automated tool, performed passive network monitoring of DPAS related network traffic over a period of 10 days and confirmed that no unencrypted traffic was transmitted</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			over commercial or wireless networks.	
47	Discretionary access controls are a sufficient IA mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rules.	<u>DISA-OKC</u> ACLs have been implemented for interconnections among DoD information systems. The ACLs are controlled by DISA-OKC.	<u>DISA-OKC</u> Confirmed through inquiry that a controlled interface was used for interconnections among the DoD information systems that were connected to DPAS. Observed the existence of the ACLs at DISA-Dayton by having a network administrator display the listing on his desktop.	No relevant exceptions noted.
48	Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures is planned, scheduled, and conducted.	<u>DISA-Ogden</u> An unannounced ISS scan is performed monthly. Automated SRR scripts are run on each server and reported to the Montgomery SRR database on a weekly basis. Each system has an SRR and an ISS scan before it is connected to the network. The DISA Field Security Office runs periodic SRRs and	<u>DISA-Ogden</u> Confirmed through inquiry that conformance testing was performed that included periodic, unannounced, in-depth monitoring and provided for specific penetration testing to confirm compliance with all vulnerability mitigation procedures was planned, scheduled, and conducted. Confirmed through inquiry that DISA-Ogden did not perform periodic network penetration	DISA-Ogden did not perform periodic network penetration testing to identify vulnerabilities with the DPAS architecture.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		ISS scans. DISA-Ogden conducts an operation facility environmental risk assessment.	testing. Inspected ISS scans and obtained evidence that the conformance and penetration testing was being completed.	
49	All users are warned that they are entering a Government information system.	<u>DISA-Ogden; DISA-Dayton</u> A warning banner notifies a user that they are entering a DoD information system when they logon.	<u>DISA-Ogden; DISA-Dayton</u> Observed that workstations display a DoD warning banner at logon.	No relevant exceptions noted.
50	Information and DoD information systems that store, process, transmit, or display data in any form or format that is not approved for public release comply with all requirements in policy and guidance documents.	<u>DISA-Ogden</u> Unless there is an overriding technical or operational problem, workstation screen-lock functionality is associated with each workstation. When activated, the screen-lock function places an unclassified pattern onto the entire screen of the workstation, totally hiding what was	<u>DISA-Ogden</u> Confirmed through observation that workstation screen-lock functionality was applied. Inquired with key personnel to confirm that information in transit through a network at the same classification level was encrypted. Using an automated tool, performed passive network monitoring of DPAS related network traffic over a period of 10 days to test for unencrypted traffic	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>previously visible on the screen.</p> <p>Information in transit through a network at the same classification level is encrypted.</p> <p>Work areas are behind monitored entrances and appropriate placement of cubicles and workstations is implemented.</p>	<p>transmitted over commercial or wireless networks.</p> <p>Observed that displays and printers used for classified information were positioned to deter unauthorized individuals from reading the information at all of the locations.</p>	
51	<p>Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography.</p>	<p><u>DISA-Ogden</u> Information in transit through a network at the same classification level is encrypted.</p>	<p><u>DISA-Ogden</u> Inquired with key personnel to confirm that information in transit through a network at the same classification level was encrypted with NIST-certified cryptography.</p> <p>Using an automated tool, performed passive network monitoring of DPAS related network traffic over a period of 10 days to test for unencrypted</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			network traffic.	
52	Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a Demilitarized Zone.	<u>DISA-Ogden</u> Connections between DoD enclaves and the Internet are configured with a Demilitarized Zone.	<u>DISA-Ogden</u> Inspected the DISA-Ogden system architecture to confirm that connections between DoD enclaves and the Internet were configured with a Demilitarized Zone.	No relevant exceptions noted.
53	Boundary defense mechanisms to include firewalls and network IDS are deployed at the enclave boundary.	<u>DISA-OKC, DISA-Dayton</u> DISA-Ogden and DISA-Dayton have boundary defense mechanisms in place that include firewalls and IDSs.	<u>DISA-OKC, DISA-Dayton</u> Inspected the DISA-OKC system architecture to confirm that boundary defense mechanisms to include firewalls and network IDS were deployed at the enclave boundary. Read system network diagram and corroborated with the System Administrator to confirm that defense mechanisms were employed. Observed the existence of firewalls and IDSs.	No relevant exceptions noted.
54	Devices that display or output classified or sensitive information in	<u>DISA-Ogden</u> Work areas are behind monitored entrances and	<u>DISA-Ogden</u> Observed that displays and printers were used for classified information	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	<p>human-readable form are positioned to deter unauthorized individuals from reading the information.</p>	<p>appropriate placement of cubicles and workstations is implemented.</p>	<p>and confirmed that these items were positioned to deter unauthorized individuals from reading the information at all of the locations.</p>	
<p>55</p>	<p>Individuals requiring access to sensitive information are processed for access authorization in accordance with DoD personnel security policies.</p>	<p><u>DISA-Ogden</u> A Form 2875 is required to be completed by anyone requesting access to DPAS. The form must be completed correctly and have all the required signatures.</p>	<p><u>DISA-Ogden</u> Read the policies and procedures for gaining access to sensitive information.</p> <p>Inspected a haphazard sample of SAAR Form 2875s to confirm that each Form 2875 detailed the user's justification for access, security clearance level, and that each Form 2875 was properly approved.</p>	<p>We noted that 4 out of 45 users tested did not have a System Access Authorization Request form on file. According to DISA-Ogden personnel, these missing forms resulted from the transfer of responsibility for the forms from DISA-Dayton to DISA-Ogden. DISA-Ogden believed they were lost during the physical transfer of the forms from DISA-Dayton to DISA-Ogden. The DISA-Ogden Contract Technical Requirement Analyst</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				<p>indicated to us that these four users were authorized to have access to the system based on daily interaction processing authorization requests. Confirmed through inquiry of the IT Specialist, User Creation Division, and observed a sample of user access forms to that DPAS user accounts and necessary documentation was on file.</p>
56	<p>DoD information systems comply with DoD ports, protocols, and services guidance.</p>	<p><u>DISA-Dayton</u> All port, protocols, and services used by DPAS are in compliance with DoD standards documented in the Unix STIG.</p>	<p><u>DISA-Dayton</u> Confirmed through the performance of network monitoring that DoD information systems complied with DoD ports, protocols, and services guidance, including all ports, protocols, and services whether currently active or planned for use.</p> <p>Confirmed that all ports, protocols, and services were identified and</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>registered.</p> <p>Read the documentation of DPAS being successfully STIGed.</p>	
57	Binary or machine executable public domain software products and other software products with limited or no warranty are not used in DoD information systems.	<p><u>DISA-Ogden</u> DPAS does not have binary or machine executable public domain software installed.</p>	<p><u>DISA-Ogden</u> Read a listing of software products used at DISA-Ogden to confirm DPAS did not have binary or machine executable public domain software installed.</p> <p>Read software inventory listing and conducted inquiry with the Program Manager for Configuration Management to confirm that binary or machine executable public domain software products and other software products with limited or no warranty were not installed on DPAS.</p>	No relevant exceptions noted.
<i>Application Software Development and Change Control</i>				
58	A system development life cycle methodology (SDLC) has been implemented and documented.	<p><u>NAVSISA</u> A Change Management Plan has been implemented, documented, and</p>	<p><u>NAVSISA</u> Read the Change Management Plan to confirm that it had been updated.</p>	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>updated. NAVSISA follows a documented Software Configuration Management Plan for all system maintenance activity.</p>		
59	<p>Authorizations for software modifications are documented and maintained.</p>	<p><u>NAVSISA</u> Using the DPAS Software Configuration Management Plan as the overarching guidance, all System Change Requests (SCRs) are approved by the DPAS Program Manager. Specific changes that are to occur as a result of SCRs are documented in the System Subsystem Specification that is developed by NAVSISA and provided to the Software Director for approval. Changes relating to PTRs are also approved by the Software Director. Configured Items (CIs)</p>	<p><u>NAVSISA</u> Selected the full population of 48 code and database modifications that occurred during the seven month period under review (September 2004 to March 2005) from the DPAS production code library (UNIX directory) and traced each modification to an approved SCR or PTR and confirmed through inspection that it had been authorized by the Program Manager or Software Director and traced each SCR or PTR identified above to the Release Authorization Report to confirm that the CIs had been approved by the Software Director.</p> <p>Inquired of key NAVSISA personnel and DPAS users to confirm the results of the testing</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>related to SCRs and PTRs that are identified for a release are tracked at NAVSISA using CMTS. CMTS provides visibility at the individual CI level as to specific changes that are being prepared for any given release. Prior to a release, a Release Authorization Report is prepared that identifies the CIs that are contained in the release. The DPAS Software Director and a representative of NAVSISA sign this report attesting to the CIs that are to be released to production.</p>	<p>above.</p>	
60	<p>Use of public domain and personal software is restricted.</p>	<p><u>DFAS-Columbus</u> Public domain and personal software must be approved for use.</p>	<p><u>DFAS-Columbus</u> Read DPAS SSAA to confirm that personal software was restricted.</p> <p>Read inventory listing to confirm</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>that binary or machine executable public domain software products and other software products with limited or no warranty were not installed on DPAS.</p>	
61	<p>Changes are controlled as programs progress through testing to final approval.</p>	<p><u>NAVSISA</u> Test plan standards have been developed for all levels of testing that define responsibilities for each party including users, system analysts, programmers, auditors, quality assurance, and library control.</p> <p>Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.</p> <p>Software changes are documented so that they</p>	<p><u>NAVSISA</u> Using the same sample selected for control objective 59, confirmed that the change followed the appropriate test and migration process by inspecting the following for completeness and authorization:</p> <ul style="list-style-type: none"> ○ System Test Plan; ○ Detailed system specifications; and ○ Unit, System and Acceptance testing results. <p>Inquired of key NAVSISA personnel and DPAS users to confirm the results of the testing above.</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>can be traced from authorization to the final approved code and they facilitate “trace-back” of code to design specifications and functional requirements by system testers.</p> <p>Unit, integration, and system testing are performed and approved 1) in accordance with the test plan and, 2) applying a sufficient range of valid and invalid conditions.</p> <p>A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing.</p> <p>Live data are not used in the testing of program</p>		

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>changes except to build test data files.</p> <p>Test results are reviewed and documented.</p> <p>Program changes are moved into production only upon documented approval from users and system development management.</p> <p>Documentation is updated for software, hardware, operating personnel, and system users when a new or modified system is implemented.</p>		
62	<p>Emergency changes are promptly tested and approved before being moved into production.</p>	<p><u>NAVSISA</u> Using the DPAS Software Configuration Management Plan as the overarching guidance, all SCRs are approved by</p>	<p><u>NAVSISA</u> Selected the full population of 48 code and database modifications that occurred during the seven month period under review (September 2004 to March 2005)</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>the DPAS Program Manager. Specific changes that are to occur as a result of SCRs are documented in the System Subsystem Specification that is developed by NAVSISA and provided to the Software Director for approval. Changes relating to PTRs are also approved by the Software Director. CIs related to SCRs and PTRs that are identified for a release are tracked at NAVSISA using the CMTS. CMTS provides visibility at the individual CI level as to specific changes that are being prepared for any given release. Prior to release, a Release Authorization Report is prepared that identifies the CIs that are</p>	<p>from the DPAS production code library (UNIX directory) and traced each modification to an approved SCR or PTR and confirmed through inspection that it had been authorized by the Program Manager or Software Director and traced each SCR or PTR identified above to the Release Authorization Report to confirm that the CIs had been approved by the Software Director.</p> <p>Inquired of key NAVSISA personnel and DPAS users to confirm the results of the testing above.</p> <p>Using the same sample selected above, confirmed that the change followed the appropriate test and migration process by inspecting the following for completeness and authorization:</p> <ul style="list-style-type: none"> ○ System Test Plan (STP); ○ Detailed system specifications; and ○ Unit, System and 	

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>contained in the release. The DPAS Software Director and a representative of NAVSISA signs this report attesting to the CIs that are to be released to production.</p> <p>Test plan standards have been developed for all levels of testing that define responsibilities for each party including users, system analysts, programmers, auditors, quality assurance, and library control.</p> <p>Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.</p>	<p>Acceptance testing results.</p> <p>Inquired of key NAVSISA personnel and DPAS users to confirm the results of the testing above.</p>	

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>Software changes are documented so that they can be traced from authorization to the final approved code and they facilitate “trace-back” of code to design specifications and functional requirements by system testers.</p> <p>Unit, integration, and system testing are performed and approved 1) in accordance with the test plan and, 2) applying a sufficient range of valid and invalid conditions.</p> <p>A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing.</p>		

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>Live data are not used in testing of program changes except to build test data files.</p> <p>Test results are reviewed and documented.</p> <p>Program changes are moved into production only on documented approval from users and system development management.</p> <p>Documentation is updated for software, hardware, operating personnel, and system users when a new or modified system is implemented.</p>		
63	<p>Distribution and implementation of new or revised software is controlled.</p>	<p><u>NAVSISA</u> A Release Authorization Report is prepared that identifies the CIs that are contained in the release</p>	<p><u>NAVSISA</u> Using the same sample selected for control objective 59, confirmed that the change followed the appropriate distribution process by inspecting the Release Authorization Report</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		and approves the release for distribution.	for completeness and authorization. Inquired of key NAVSISA personnel and DPAS users to confirm the results of the testing above.	
64	Programs are labeled and inventoried.	<u>NAVSISA</u> Major release CIs for CCB approved SCR's are entered into CMTS using the impact cost analysis forms for each SCR. All additions, changes, or deletions to the production baseline SCR are submitted to the Change Management for approval. All CIs are assigned identification numbers.	<u>NAVSISA</u> Using the same sample selected for control objective 59, confirmed that the CI that was changed had been approved, labeled, assigned an ID, and inventoried in CMTS. Inquired of key NAVSISA personnel and DPAS users to confirm the results of the testing above.	No relevant exceptions noted.
65	Access to program libraries is restricted to appropriate personnel.	<u>NAVSISA</u> Authorized individuals are restricted to only specifically assigned libraries by the DPAS Librarian.	<u>NAVSISA</u> Observed the DPAS Librarian to demonstrate how the development and production libraries were controlled. Inspected the ACLs for the Production and Development	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>libraries (directories) to confirm that only authorized personnel had access.</p> <p>Observed a system developer attempt to update the production library to confirm that access to the production library was restricted.</p> <p>Inquired of key NAVSISA personnel and DPAS users to confirm the results of the testing above.</p>	
66	<p>Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities.</p>	<p><u>NAVSISA</u> The contract agreement (GS-07T-00-BGD-0063) and Statement of Work with General Dynamics, who performs code development services for NAVSISA in support of DPAS, expressly addresses task, required skill sets, security investigations and nondisclosure agreements for the</p>	<p><u>NAVSISA</u> Inspected the General Dynamics contract agreement to confirm if it expressly addressed Government, service provider and end-user IA roles and responsibilities.</p> <p>Inquired of key NAVSISA personnel and DPAS users to confirm the results of the testing above.</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		support of DPAS services.		
67	The acquisition of all IA- and IA-enabled GOTS IT products is limited to products that have been evaluated by the NSA or in accordance with NSA-approved processes.	<u>DISA-OKC</u> All IA devices have been approved by NSA or in accordance with NSA approval processes before acquiring and implementing.	<u>DISA-OKC</u> Confirmed through inquiry that DISA-OKC verified that all IA related products were approved by NSA or in accordance with NSA approved processes. Inspected the NIAP website and confirmed that the website provided a list of approved products including the products used by DPAS.	No relevant exceptions noted.
68	Movement of programs and data among libraries is controlled.	<u>NAVSISA</u> A Release Authorization Report is prepared that identifies the CIs that are contained in the release and approves the release for distribution.	<u>NAVSISA</u> Using the same sample selected for control objective 59, confirmed that the changes selected for testing followed the appropriate distribution process by inspecting the Release Authorization Report for completeness and authorization. Inquired of key NAVSISA personnel and DPAS users to confirm the results of the testing	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
69	<p>Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability, such as buffer overruns, are specified for all software development initiatives.</p>	<p><u>DFAS-Columbus</u> The DPAS Security Specialist at DFAS-Columbus receives DPAS Release Notes from NAVSISA-Mechanicsburg. The DPAS Security Specialist then reviews the DPAS Release Notes for changes related to security. The Testing Director at NAVSISA-Mechanicsburg develops test plans for testing security-related changes. The DPAS Security Specialist then reviews these test plans and assists in the testing of security-related changes included in the DPAS Release.</p> <p><u>NAVSISA</u> Test plan standards have been developed for all</p>	<p>above.</p> <p><u>DFAS-Columbus</u> Inquired of DPAS Security Specialist at DFAS-Columbus as to his roles and responsibilities for the release of security-related changes included in DPAS Releases.</p> <p>Observed release notes for all major DPAS production releases that occurred during the audit period at NAVSISA-Mechanicsburg.</p> <p><u>NAVSISA</u> Using the same sample selected for control objective 59, confirmed that the change followed the appropriate test and migration process by inspecting the following for completeness and authorization:</p> <ul style="list-style-type: none"> ○ System Test Plan; ○ Detailed system specifications; and ○ Unit, System and Acceptance testing results. <p>Inquired of key NAVSISA</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, and library control).</p>	<p>personnel and DPAS users to confirm the results of the testing above.</p>	
<i>System Software Controls</i>				
70	<p>Access authorizations are appropriately limited.</p>	<p><u>DISA-OKC, DISA-Ogden</u> ACLs, user management controls, firewalls, IDS, and authentications are used to control network access.</p> <p>Users must have the same level of access of the system they are trying to access, have an established username and password, and be allowed through the router and firewall.</p>	<p><u>DISA-OKC</u> Read the policies and procedures for restricting access to the systems software to confirm that they were up-to-date.</p> <p><u>DISA-Ogden</u> Obtained a list from the Discretionary Access Control of all individuals who had direct access to the system software and selected a haphazard sample of Ogden users with direct access. For each user selected, confirmed with key management personnel that these users were authorized to have this access.</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
71	<p>All access paths have been identified and controls implemented to prevent or detect access for all paths.</p>	<p><u>DISA-OKC</u> The following are used to provide telecommunication controls:</p> <ul style="list-style-type: none"> • ACLs • IDS • Firewalls • Encryption, and • Network monitoring. <p>ACLs have been implemented for interconnections among DoD information systems. The ACLs are controlled by DISA-OKC.</p>	<p><u>DISA-OKC</u> Through observation and inquiry, confirmed that telecommunications controls were properly implemented.</p> <p>Obtained policy and procedures relating to DoD information systems access controls to confirm they existed.</p> <p>Through observation and inquiry, confirmed that a controlled interface was used for interconnections among the DoD information systems that were connected to DPAS.</p> <p>Observed the existence of ACL, IDS, Firewalls, Encryption, and Network monitoring.</p> <p>Reviewed output on computer monitor and conducted inquiry of IT Specialist.</p>	<p>No relevant exceptions noted.</p>
72	<p>Policies and techniques have been implemented</p>	<p><u>DISA-Ogden</u> The system utilities that</p>	<p><u>DISA-Ogden</u> Inquired with key Ogden personnel</p>	<p>Standard Operating Procedures and DISA-</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	for using and monitoring the use of system utilities.	<p>support DPAS are limited to root access only.</p> <p>Policies and procedures for using and monitoring the use of system software utilities exist and are up-to-date.</p> <p>Responsibilities for using sensitive system utilities have been clearly defined and are understood by systems programmers.</p> <p>Responsibilities for monitoring use are defined and understood by technical management.</p> <p>The use of sensitive system utilities is logged using access control software reports or job accounting data.</p>	<p>to confirm how root access was administered. Obtained the list of individuals with root access and conferred with Management that access was appropriate and that the use of accounts with root access was logged.</p> <p>Read the policies and procedures for the monitoring of systems software to confirm that they existed and were current.</p> <p>Read a sample of the audit logs from the DPAS servers to confirm that key Ogden personnel reviewed the logs on a regular basis and that any issues noted were documented and researched.</p>	<p>Ogden SSAA were not updated to reflect current processes and procedures.</p> <p>In addition, DISA-Ogden did not proactively monitor or review audit trails since it did not have the tools to perform such monitoring.</p> <p>During our fieldwork, we noted that standard operating procedures had been subsequently documented.</p>
73	System software changes	<u>DISA-Dayton</u>	<u>DISA-Dayton</u>	No relevant exceptions

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	<p>are authorized, tested, and approved before implementation.</p>	<p>DPAS system software patches and upgrades are applied in accordance with Information Assurance Vulnerability Alert bulletins or DISA-Ogden policy unless otherwise noted in the Service-Level Agreement (SLA).</p> <p>Current policies and procedures exist for identifying, selecting, installing, and modifying system software.</p> <p>New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document.</p> <p>New system software</p>	<p>Obtained and read the change management policies and procedures for systems software to confirm that they existed and were current.</p> <p>Obtained a list of all system software purchases and modifications from September 1, 2004 through April 30, 2005 and tested the full population of modifications. For each modification, obtained the change request document for each modification and confirmed that each modification was approved by key Ogden personnel prior to implementation and that each modification was tested and the test results were approved prior to the modification being implemented.</p> <p>Obtained a list of all emergency changes implemented from September 1, 2004 through April 30, 2005 and confirmed through inspection that these changes</p>	<p>noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>versions or products and modifications to existing system software are tested and the test results are approved before implementation. All emergency changes follow the change management process and must be approved prior to implementation.</p>	<p>followed a change management process and were tested and approved prior to implementation.</p>	
74	<p>Installation of system software is documented and reviewed.</p>	<p><u>DISA-Ogden</u> DPAS system software and patch installations are tracked through HP/UX software utilities.</p> <p>Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.</p> <p>Migration of tested and approved system software to production is performed by an</p>	<p><u>DISA-Ogden</u> Confirmed through inquiry that changes to the HP/UX servers were managed and logged in the CMS.</p> <p>Using the sample of system software modification/implementations selected for control objective 73, confirmed that users were notified of the modification prior to implementation.</p> <p>Obtained the system software audit logs that showed each change selected above being implemented. Confirmed with key Ogden personnel that the logs were</p>	<p>DISA-Ogden did not have a software tool available to proactively monitor or review operating system audit trails because they did not have the appropriate tool that would allow them to efficiently analyze large volumes of audit log data to identify potential high risk and unusual system activity.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>independent source.</p> <p>Installation of all system software is logged to establish an audit trail and reviewed by management. All system software is current and has current and complete documentation.</p>	<p>reviewed.</p> <p>Obtained the list of personnel with access to migrate system software modifications from the test environment to the production environment and confirmed with Management that an appropriate individual migrated each of the selected modifications.</p> <p>Observed the presence of HP/UX software utilities on the DPAS servers.</p> <p>Read the Executive Software Inventory for DPAS to confirm that it was current.</p>	
75	<p>Good engineering practices with regards to the integrity mechanisms of Commercial off-the-Shelf, GOTS and custom developed solutions are implemented for incoming and outgoing</p>	<p><u>DISA-OKC</u> Integrity mechanisms are used for interconnections among the DoD information systems connecting to DPAS for incoming and outgoing files.</p>	<p><u>DISA-OKC</u> Confirmed through inquiry that a controlled interface was used for interconnections among the DoD information systems that were connected to DPAS.</p> <p>Observed the existence of ACL,</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	files.		<p>IDS, Firewalls, Encryption, and Network monitoring.</p> <p><u>DISA-Dayton</u> Using an automated tool, performed passive network monitoring of DPAS related network traffic over a period of 10 days to confirm that no unencrypted traffic was transmitted over commercial or wireless networks.</p> <p>Confirmed through corroborative inquiry that interfaced inputs were automatically validated by the system for missing information, format, consistency and reasonableness.</p> <p>Observed system batch files of interfaced inputs for control totals and line counts.</p>	
<i>Segregation of Duties</i>				
76	Incompatible duties have been identified and	<u>DISA-Ogden</u> System Administrator,	<u>DISA-Ogden</u> Read the DISA-Ogden	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	policies implemented to segregate these duties.	System Security, IAO and IAM duties are all separated at SMC Ogden.	organizational chart and read the job descriptions for the positions at DISA-Ogden in relation to DPAS to confirm that there was an appropriate segregation of duties and that incompatible duties did not exist.	
77	System management job descriptions have been documented.	<u>DISA-Ogden</u> Job descriptions of key DPAS system support personnel are documented.	<u>DISA-Ogden</u> Read the job descriptions for key system support personnel at DISA-Ogden to confirm they existed.	No relevant exceptions noted.
78	System management employees understand their duties and responsibilities.	<u>DISA-Ogden</u> DISA-Ogden employees understand their duties and responsibilities in accordance with DISA policies and procedures.	<u>DISA-Ogden</u> Selected a sample of employees and confirmed through inquiry that they understood their duties and responsibilities. Observed documentation to confirm that employees had signed position descriptions.	No relevant exceptions noted.
79	Management reviews effectiveness of control techniques.	<u>DFAS-Columbus</u> Management periodically assesses the appropriateness and effectiveness of control techniques by updating the Systems Security	<u>DFAS-Columbus</u> Read the DPAS Systems Security Policy, Security Requirements, and Certification Test and Evaluation Plan and Procedures to confirm that each had been updated.	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		Policy, Security Requirements, and Certification Test and Evaluation Plan and Procedures.		
80	Formal procedures guide system management personnel in performing their duties.	<u>DISA-Ogden</u> Formal procedures are documented and accessible to guide personnel in performing their duties.	<u>DISA-Ogden</u> Read Standard Operating Procedures used by DISA-Ogden personnel for performance of their job duties in respect to DPAS.	Standard operating procedures and DISA-Ogden SSAA were not updated to reflect existing processes and procedures. During our fieldwork, we noted that standard operating procedures had been subsequently documented.
81	Access procedures enforce the principles of separation of duties and “least privilege.”	<u>DFAS-Columbus</u> User Access profiles are created for DPAS users to limit access to DPAS and enforce a separation of duties.	<u>DFAS-Columbus</u> Read the access control policies and procedures for DISA-Ogden for compliance with the principles of separation of duties and “least privilege.”	No relevant exceptions noted.
82	Active supervision and review are provided for	<u>DISA-Ogden</u> A documented	<u>DISA-Ogden</u> Read the DISA-Ogden	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	all system management personnel.	management structure with supervision has been established.	organizational chart to confirm that a management structure was established. Read position descriptions of DPAS key support personnel to confirm supervisory responsibilities were established.	
	<i>Application Controls</i>			
1	Access controls have been established to enforce segregation of duties.	<u>DFAS-Columbus</u> The system design permits only authorized users to enter, modify, or otherwise alter property records. The system incorporates adequate security features that prevent unauthorized access to the property system by unauthorized individuals to provide access control. The system's design can be observed and tested in a production replica.	<u>DFAS-Columbus</u> Observed the DPAS system to confirm that its design supported segregating duties. Observed DPAS to confirm that users must possess a valid Login and Password to gain access to the system. Observed the entering of an invalid User ID and password to confirm that the system displayed an error message to the user. Observed the DPAS system to confirm that each user account was assigned a Security Profile that restricted access by module, program, UIC, and Hand Receipt.	No relevant exceptions noted.
2	Controls provide	<u>DFAS-Columbus</u>	<u>DFAS-Columbus</u>	No relevant exceptions

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	<p>reasonable assurance that all asset acquisitions are recorded.</p>	<p>The system contains edits and validations that assist the user in adequately recording beginning balances, acquisitions, and withdrawals, and it calculates ending balances expressed in values and physical units, except for heritage assets and stewardship land for which all end of period balances are expressed in physical units only.</p>	<p>Confirmed through observation that the DPAS system contained edits and validations that assisted the user in adequately entering beginning balances, acquisitions, and withdrawals through required or restricted fields. Through re-performance, attempted to proceed beyond window that contained fields without entry to confirm that system prompts user with warning message.</p>	<p>noted.</p>
<p>3</p>	<p>Controls provide reasonable assurance that all asset disposals are recorded.</p>	<p><u>DFAS-Columbus</u> The system contains edits and validations that assist the user in adequately identifying property as or as held for disposal or retirement.</p>	<p><u>DFAS-Columbus</u> Observed fields in DPAS to confirm that they provided the user the capability of indicating the asset for disposal or retirement. Observed data fields in DPAS to confirm that data entry into those data fields was required and</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>restricted to specified data values. Through re-performance, attempted to proceed beyond a window that contained fields without entry to confirm that the system prompts users with warning messages.</p>	
4	<p>Controls provide reasonable assurance that all asset acquisitions are recorded in accordance with DoD and Federal entity's policy as applicable.</p>	<p><u>DFAS-Columbus</u> The system provides users the capability of capturing and categorizing capital assets according to capitalization thresholds in compliance with federal regulation.</p>	<p><u>DFAS-Columbus</u> Confirmed through observation of the DPAS system that it had been designed to enforce the DoD Financial Management Regulation (FMR) Volume 4, Chapter 6.</p> <p>Observed the DPAS system's capitalization key fields to confirm that it provided the user the capability of categorizing the asset as a capital asset (value over \$100,000).</p> <p>Observed the DPAS system's validation messages that controlled the user's classification of an asset as a capital asset.</p> <p>Observed that the DPAS system calculated the annual amortization</p>	<p>DPAS does not calculate the annual amortization of estimated mat, clean-up costs, and the unamortized balance.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			of estimated material, clean-up costs, and the unamortized balance.	
5	Controls provide reasonable assurance that depreciation charges are valid.	<u>DFAS-Columbus</u> The system contains edits and validations that assist the user in accurately recording assets for depreciation.	<u>DFAS-Columbus</u> Observed the system to confirm that it recorded depreciation charges for assets that were subject to depreciation. Observed fields that were required and or restricted for recording assets that were subject to depreciation.	No relevant exceptions noted.
6	Controls provide reasonable assurance that asset acquisitions are accurately recorded.	<u>DFAS-Columbus</u> Asset-related transactions affecting the asset register and/or master file are edited and validated to prevent duplication and reduce the likelihood of creating erroneous property records to maintain the integrity of data recorded in the system; identified errors are	<u>DFAS-Columbus</u> Read DPAS SSAA Appendix D to confirm that DPAS contained technical controls over user access, authorization, data integrity, and data validation. Observed the DPAS system to confirm that it included editing and validation functions that would not permit duplication of a stock number or serial number combination, or a duplicate	No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>corrected promptly.</p> <p>The system contains edits and validations that assist the user in accurately capturing the method and costs of acquiring each property item or bulk property items including direct purchase, completed work-in-process, completed internal user software in development, capital lease, donation, loan, grant, non-reciprocal transfer or reciprocal transfer, and the date of the acquisition.</p>	<p>barcode.</p> <p>Observed the stock number, serial number, and barcode fields to confirm that the user was prompted with an error message if the user entered a duplicate value.</p> <p>Observed that significant error messages, such as system aborts, were logged to an error log file and observed that the History Table captured asset transactional activity.</p> <p>Observed edits and validations were built into the system. Confirmed through observation that the system prompted users with warning messages when values were not entered into required fields.</p> <p>Observed the application's Hand Receipt Module to confirm that it provided the user the capability of capturing the method of asset acquisition with the assignment of</p>	

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>the appropriate “Action Code” and “Date of Acquisition” when performing an “End Item Increase.”</p> <p>Observed that fields “Acquisition Date” and “Action Code” that allow a user to capture the method of asset acquisition, to confirm that the fields were required and restricted. Through re-performance, attempted to proceed beyond a window that contained Acquisition Date and Action Code without entry to confirm that the system prompted the user with a warning message.</p>	
7	<p>Controls provide reasonable assurance that asset disposals are accurately calculated and recorded in accordance with USSGL policy.</p>	<p><u>DFAS-Columbus</u> The system calculates gain or loss at time of disposal or retirement, sale, exchange, or donation.</p> <p>The system for capitalized property classifies Property Plant & Equipment according</p>	<p><u>DFAS-Columbus</u> Read the DPAS Help Manual to confirm that the system calculates a gain or loss at the time of disposal.</p> <p>Observed the DPAS system to confirm that it provided a financial transaction for calculation of gain or loss at the time of disposal or retirement, sale, exchange, and donation.</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>to the USSGL and generates data for the journal entries necessary for recording changes in the valuation including any associated gains or losses.</p>	<p>Observed that the transaction was logged in the History Table, indicating transaction date, time, and the User ID of the person entering the transaction.</p> <p>Re-performed test and gain or loss calculations similar to depreciation re-performance tests to confirm that a gain or loss was accurately calculated.</p> <p>Observed the system to confirm that its configuration performed a cross-walk to the USSGL.</p> <p>Observed the application's asset code field to confirm that it provided the user the capability of classifying PP&E according to the USSGL.</p> <p>Observed the asset code field to confirm that it was a required or restricted field. Through re-</p>	

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>performance, attempted to proceed beyond a window that contained the asset code field without an entry to confirm that the system prompted users with a warning message.</p>	
8	<p>Controls provide reasonable assurance that depreciation charges are accurately calculated and recorded.</p>	<p><u>DFAS-Columbus</u> The system contains edits and validations that assist the user in aggregating like items into pools for purposes of calculating depreciation; allows users to reassign an average useful life and acquisition cost; and maintains original unique property records for pooled items.</p> <p>The system supports an appropriate depreciation method, such as straight line, physical usage and the components needed to calculate depreciation, amortization, or</p>	<p><u>DFAS-Columbus</u> Read the electronic DPAS Help Manual to confirm that the Asset Control Code (ACC) identified the accounting class of assets and that DPAS had capital threshold limits. Observed the application's Hand Receipt module and Catalog module to confirm that they provided the user the capability to aggregate homogeneous assets into asset pools via the ACC code field.</p> <p>Observed that ACC code was a required and restricted field. Through re-performance, attempted to proceed beyond a window without entering an ACC code to confirm that the system prompted users with warning a message.</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>depletion expense including: original asset value; estimated useful life; and salvage or residual value.</p> <p>The system notifies the user if information is needed for depreciation, amortization or depletion calculations when thresholds are exceeded.</p> <p>Standard programmed algorithms perform depreciation calculations.</p>	<p>Read Help Manual to confirm that it included an entire list of system permitted ACC codes.</p> <p>Observed the application's Catalog module and Accounting module to confirm that they provided the user the capability of capturing the estimated useful life, depreciation, amortization, depletion method, and salvage or residual value for each asset or group of assets when applicable and that the system supported only the straight-line calculation method.</p> <p>Observed the DPAS system to confirm that it prompted users with the warning message "Threshold Exceeded" if value exceeded system's configured threshold.</p> <p>Re-performed depreciation algorithm for a haphazard sample of transactions to confirm correct calculation was being routinely</p>	

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
9	<p>Controls provide reasonable assurance that recorded asset acquisitions represent assets acquired by the organization.</p>	<p><u>DFAS-Columbus</u> The system contains edits and validations that prevent the user from entering erroneous data for the acquisition of property in-transit.</p>	<p>performed. <u>DFAS-Columbus</u> Observed the application's Hand Receipt module to confirm that it provided the user the capability of identifying an asset as Inbound, Outbound, or Not Applicable by assigning the appropriate "In-transit Code." Observed that the In-transit Code field restricted the user to selecting one of the three options and defaulted to "Not Applicable."</p> <p>Observed the application's Catalog and Document Register to confirm that they provided users the capability of tracking the In-transit Code of an asset by storing the asset's Contract Number. Observed that the Contract Number field could be pre-populated by Fed Log or populated by user entry and that this field was not restrictive. Observed the fields "In-transit Code" and "Contract Number" to confirm that they were required or</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>restricted. Through re-performance, attempted to proceed beyond a window that contained a Contract Number without an entry to confirm that the system prompted users with warning messages.</p>	
<p>10</p>	<p>Controls provide reasonable assurance that only valid changes are made to the asset register and master file.</p>	<p><u>DFAS-Columbus</u> Personnel who are responsible for asset transaction processing have neither responsibility for asset master file maintenance nor update access to the asset master file.</p>	<p><u>DFAS-Columbus</u> Read the DPAS SSAA Appendix O, “DPAS Security Awareness Guide,” to confirm that the roles and responsibilities were defined for the System Administrator, IAO, Site Security Officer, and Users.</p> <p>Observed documentation that defined user roles and responsibilities.</p> <p>Observed the application to confirm that users must possess a valid Login and Password to gain access to the system.</p> <p>Observed that each user account was assigned a Security Profile that</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>restricted access by module, program, UIC, and Hand Receipt.</p> <p>Observed documentation and communication between the PBO and the Information Systems Security Officer responsible for setting up Security Profile that dictated which modules and functions each user had access to.</p>	
11	<p>Controls provide reasonable assurance that erroneous transactions are identified without being processed and without undue disruption of the processing of other valid transactions.</p>	<p><u>DISA-Dayton</u> Transactions that are reprocessed are controlled in a similar manner to the original transactions with appropriate modifications (for both business process and security controls). The system provides an audit trail of all transactions processed, transaction errors, error descriptions, and error correction procedures.</p>	<p><u>DISA-Dayton</u> Confirmed through inquiry that erroneous transactions were reprocessed in a similar manner to the original transactions.</p> <p>Read Standard Operating Procedures to confirm that documented procedures existed for monitoring transaction processing.</p> <p>Observed that transactions were reprocessed in a manner similar to original transactions.</p> <p>Observed the batch status file to confirm that erroneous transactions</p>	<p>No standard operating procedures existed for monitoring transaction processing. In addition, error correction procedures were not documented and maintained. Finally, the majority of the transaction processing, monitoring, and error correction functions were performed by one individual at DISA who was the only person who had the full technical knowledge of DPAS to perform all of the</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>were monitored, identified, and corrected.</p> <p>Observed the batch status file to confirm that it recorded all successful and unsuccessful batches.</p> <p>Observed the Batch Error History report and descriptions to confirm that erroneous transactions were monitored, identified, and corrected and that correction procedures were recorded.</p>	<p>functions. The unavailability of this person could impact the timeliness and quality of system transaction file processing.</p>
12	<p>Controls provide reasonable assurance that transaction data entered for processing via automated interface are subject to a variety of controls to check for accuracy, completeness and validity and that input data are validated and edited as close to the point of origination as possible.</p>	<p><u>DISA-Dayton</u> Interfaced inputs are automatically validated by the system for missing information, format, consistency and reasonableness. Checks for valid information are made when inputs are received. Transactions failing edit and validation routines are posted to a suspense file and reported. Where a</p>	<p><u>DISA-Dayton</u> Confirmed through inquiry that interfaced inputs were automatically validated by the system for missing information, format, consistency and reasonableness. Observed the application to confirm that it would reject and not process erroneous transactions. Observed log files that confirm the logging of successful and unsuccessful transactions between</p>	<p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>file contains valid and invalid transactions, processing of valid transactions is not delayed.</p> <p>Interfaced inputs are transmitted in batch files and batch control totals are used to balance sent transactions to received transactions. Out-of-balance conditions are reported, corrected and reentered.</p>	<p>interfaces.</p> <p>Observed the error file to confirm that erroneous transactions were monitored, identified, and corrected.</p> <p>Observed system batch files of interfaced inputs for control totals and line counts.</p> <p>Observed the suspense file to confirm that erroneous transactions were monitored, identified, and corrected.</p> <p>Inspected a haphazard sample of batch transaction errors to confirm that all 7 transaction errors were corrected.</p> <p>Observed that rerun transactions were subjected to the same quality review as the original transactions.</p>	

**Section IV: Supplemental Information Provided by the Defense
Information Systems Agency**

IV. Supplemental Information Provided by the Defense Information Systems Agency

This section has been prepared by DISA and is included to provide user organizations with information DISA believes will be of interest to such organizations but is not covered in the scope or control objectives established for the Statement on Auditing Standards 70 review. Specifically included is a summary of procedures that DISA has put into place to enable recovery from a disaster affecting the DISA location where DPAS is housed and maintained.

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 DoD OIG expresses no opinion regarding the completeness and accuracy of this information.

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 Continuity of Operations support agreement between DPAS 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 DPAS processing.

The enterprise backup process is managed by the DISA-Oklahoma City Storage Team. Backup tapes containing the incremental daily and the complete weekly backups are created at Dayton with DISA-Oklahoma City oversight. The tapes are rotated off-site to Data Storage Centers in Cincinnati, OH, for storage on a predetermined schedule.

The Crisis Management Team (CMT) at DISA-Ogden is responsible for declaring that a disaster has occurred and to initiate the Business Continuity Plan. The CMT will then activate the following response teams: Communications Team, Recovery Coordination Team, Site Recovery Team, and the Crisis Support Team (CST). In the event of disaster recovery when the DISA-Oklahoma City or DISA-Ogden sites are not available to restore the data, the DPAS customer has to request DISA-Dayton personnel to initiate the data restore process. 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. DPAS personnel and select user sites participate in the yearly Continuity of Operations test to ensure that the process works correctly and that documentation is updated appropriately.

Acronyms and Abbreviations

ACC	Asset Control Code
ACL	Access Control List
ADP	Automated Data Processing
CCB	Configuration Control Board
CI	Configured Items
CMTS	Configuration Management Tracking System
DAA	Designated Approving Authority
DECC	Defense Enterprise Computing Center
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DISA OKC	DISA Oklahoma City
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DoD OIG	Department of Defense Office of Inspector General
DPAS	Defense Property Accountability System
FSO	Field Security Operations
GOTS	Government off-the-Shelf
HP/UX	Hewlett Packard/Unix
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
ID	Identification
IDS	Intrusion Detection System
ISS	Internet Security Systems
IT	Information Technology
MAC	Mission Assurance Category
NAVSISA	Naval Supply Information Systems Activity
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PBO	Property Book Officer
PDCD	Portable Data Collection Devices
PTR	Program Trouble Report
SAAR	System Authorization Access Request
SCR	System Change Request
SMC	System Management Center
SRR	System Readiness Review
SSAA	System Security Authorization Agreement
STIG	Security Technical Implementation Guide
TASO	Terminal Area Security Officer
UIC	Unit Identification Code

ULLS-S4	Unit Level Logistics System-Supply
USSGL	United States Government Standard General Ledger
VMS	Vulnerability Management System
VPN	Virtual Private Network

Report Distribution

Office of the Secretary of Defense

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

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy
Commanding Officer, Naval Supply Information Systems Activity

Combatant Command

U.S. Joint Forces Command

Other Defense Organizations

Defense Finance and Accounting Service
Defense Information Systems Agency

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
General Accountability Office

Congressional Committees and Subcommittees, Chairman and Ranking Minority Members

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on 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, Department of Defense Office of Inspector General produced this report.

Paul J. Granetto
Patricia A. Marsh
Addie M. Beima
Kenneth H. Stavenjord
Yolanda C. Watts
LTC Shurman Vines
Jackie J. Vos
William Zeh
Charles Dekle
Kimberly D. Brothers
Michael E. Williams