August 26, 2005

Information Technology Management

Report in Defense Business Management System Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004 through May 15, 2005

(D-2005-104)

Department of Defense
Office of Inspector General

Quality *Integrity* *Accountability*

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

August 26, 2005

MEMORANDUM FOR THE OFFICE OF THE UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on Defense Business Management System Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004 through May 15, 2005 (Report No. D-2005-104)

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

We appreciate the courtesies extended to the staff. Questions should be directed to Mr. Michael Perkins at (703) 325-3557 (DSN 221-3557) or Donna Roberts at (703) 428-1070 (DSN 328-1070).

By direction of the Deputy Inspector General for Auditing:

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

Table of Contents

Foreword

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

The Department of Defense Office of the 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 DBMS directly affect 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.

DBMS is a legacy general ledger financial management system implemented at DFAS-Columbus, Ohio in 1969. DBMS has been modified significantly since 1969 with the addition of modules and subsystems to support: cost accounting, military personnel costing, funds appropriation, and reimbursable receivables. It provides support to various DoD agencies. Due to a recent migration, DBMS mid-tier servers and mainframe have been moved to DISA Systems Management Center-Ogden, Utah as of February 2005.

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

Section I: Independent Service Auditor's Report

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

August 26, 2005

MEMORANDUM FOR THE OFFICE OF THE UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on Defense Business Management System Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004 through May 15, 2005

We have examined the accompanying description of the general computer and application controls related to the Defense Business Management System (DBMS) (Section II). The DBMS, including general computer and application controls, is directly supported and maintained by DFAS and DISA. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the controls at DFAS and DISA that may be relevant to a DBMS user organization's internal controls as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and user organizations applied the controls contemplated in the design of controls at DFAS and DISA; and (3) such controls had been placed in operation as of May 15, 2005.

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

In our opinion, the accompanying description of the general computer and application controls at DFAS and DISA related to DBMS (Section II) presents fairly, in all material respects, the relevant aspects of the controls at DFAS and DISA that had been placed in operation as of May 15, 2005, including the completed migration of the DBMS application from DECC-Columbus to SMC-Ogden February 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 and DISA.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Section III, to obtain evidence about their effectiveness in meeting the related control objectives described in Section III during the period October 1, 2004 to May 15, 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 DBMS user organizations and their auditors for consideration when making assessments of control.

A number of controls in place to ensure compliance with DoD information assurance policies, including DoDI 8500.2 and Defense 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. As discussed in Section III, Control Objectives, Control Activities, and Service Auditor's Tests of Operating Effectiveness, we identified deficiencies relating to the operating effectiveness of controls in operation for the period October 1, 2004 to May 15, 2005.

In performing our examination, we found DFAS did not have policies and procedures in place for performing periodic recertification of user access to DBMS. Also, maintenance of access request forms and worksheet documents was inconsistent, resulting in separated employees maintaining access to the application. We also found that DFAS did not have policies and procedures that detailed the retention and review of DBMS access and audit logs.

Tests of operating effectiveness for general controls identified primary deficiencies in access and system software controls. Specifically:

- DECC-Columbus did not have policies and procedures requiring privileged users to only use privileged access to perform their functions. For example, Systems Administrators were not required to have a separate or additional logon to perform their non-privileged functions. Other than the supervisor, there was no one at DECC-Columbus responsible for tracking privileged role assignments. When an employee changed jobs within DECC-Columbus, there was no check to ensure the access level was adjusted to reflect current requirements.
- DECC-Columbus did not adhere to the DoD Security Technical Implementation Guide (STIG) for Resource Access Control Facility (RACF). Specifically, testing revealed there was no written standard identifying needed access. This prevented system administrators from restricting access based on position description, least privilege, and separation of duties.
- SMC-Ogden did not adhere to the Oracle STIG. Specifically, user privileges were not periodically reviewed, non-administrator accounts were granted excessive privileges, and password parameters did not comply with DoD requirements.

Tests of operating effectiveness for application controls identified primary deficiencies in authorization, completeness, and change controls. Specifically:

- DFAS did not have authorization controls in place to verify that supervisors properly assigned function codes to promote separation of duties. In addition, password configurations restricting access to DBMS did not comply with DoD length, complexity, re-use, and encryption requirements. The minimum and maximum password change period was not specified.
- Applications interfacing with DBMS sent data in clear text via File Transfer Protocol (FTP) that was not secured by encryption. In addition, the interface control for SRD-1 required a header and trailer for DBMS to accept the transaction file. However, on three separate tests, the transaction file was accepted each time without the trailer.
- The documented change control process for DBMS did not reflect existing change control processes being followed. DFAS did not have documentation supporting changes (normal and emergency), changes did not have appropriate signatures, and test plans and results were not in the change package.
- DFAS did not have Information Assurance (IA) roles specified in writing.

As a result of these deficiencies, the controls for DBMS did not provide reasonable assurance that the following control objectives were fully achieved during the period of October 1, 2004 to May 15, 2005:

- "Resource owners have identified authorized users and their access authorized," (Control Activity AC-2.1)
- "Adequate logical access controls have been implemented. Logical controls over data files and software programs," (Control Activity AC-3.1a)
- "Adequate logical access controls have been implemented. Logical controls over a database," (Control Activity AC-3.2c)
- "Access authorizations are appropriately limited," (Control Activity SS-1.1)
- Policies and techniques have been implemented for using and monitoring use of system utilities," (Control Activity SS-2.1)
- "Inappropriate or unusual activity is investigated and appropriate actions taken," (Control Activity SS-2.2)
- "Authorizations for software modifications are documented and maintained," (Control Activity CC-1.2)
- "Emergency changes are promptly tested and approved," (Control Activity CC-2.2)
- "Data entry terminals are secured and restricted to authorized users," (Control Activity AN-2.1)
- "Users are limited in what transactions they can enter," (Control Activity AN-2.2)

- "Reconciliations show the completeness of data processed at points in the processing cycle," (Control Activity CP-2.1)
- "Reconciliations show the completeness of data processed for the total cycle," (Control Activity CP-2.2) and

  "Rejected transactions are controlled with an automated error suspense file." (Control Activity AY-3.1)

In our opinion, except for the matters listed 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 October 1, 2004 to May 15, 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 listed in Section III.

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

The description of controls at DFAS and DISA is as of May 15, 2005, and the information about tests of the operating effectiveness of specific controls covers the period from October 1, 2004 to May 15, 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 controls in existence. The potential effectiveness of specific controls at DFAS and DISA is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by management of DFAS and DISA, the DBMS 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 Business Management System Operations and Controls Provided by the Defense Finance and Accounting Service

II. Description of Defense Business Management System Operations and Controls Provided by the Defense Finance and Accounting Service

A. Overview of DBMS

System Overview

DBMS was developed in incremental parts beginning with the Payroll Subsystem in 1969 and Personnel Subsystem in 1972. The Resource Administration Subsystem (RAS) was added in 1975 to support business areas such as Cost Accounting, Managerial Reporting, Military Personnel Costing, and Performance Productivity. The Appropriation Accounting Subsystem (AAS) was added in 1986 to provide a uniform, automated system of accounting for appropriated funds with major components of this subsystem being funds control, appropriation record maintenance, job order accounting, and financial reporting. Finally, the Automated Billing System (ABS) was added in 1998 to provide a centralized point of input for data needed to record and manage work requests received from customers via the reimbursable order process. After DoD selected DCPS for Payroll and Defense Civilian Personnel Data System for Personnel, the DBMS Payroll and Personnel Subsystems were eliminated. Both were decommissioned before 2000.

System Capabilities

DBMS is currently a logical partition (LPAR) on a Z890-A-04 mainframe at SMC-Ogden. It is subdivided into 17 production copies of the DBMS SUPRA database with one test database. The 17 copies support approximately 4,720 customers in the Defense Agencies Accounting Business Line spread across 60 sites. Each production database is managed separately; however, some customers manage multiple databases. The breakdown is presented below:

Customer	Number of Databases
Defense Commissary Agency	3
Defense Contract Audit Agency	1
Defense Contract Management Agency	1
Defense Finance and Accounting Service (Residual Data)	2
Defense Logistics Agency	8
Navy	2

As established by the Service Level Agreement (SLA) between DISA and DFAS, each database copy is permitted to remain online for processing only during a prescribed window. At all other times, the databases are taken offline for batch processing and maintenance purposes, prohibiting user access.

Each subsystem includes the following functions:

- RAS
    - Labor Processing – Obtains payroll and personnel data from interfacing systems that provide estimated hours and dollars for civilian employees.
    - Organizational Management – Establishes controls that impose hierarchical relationships between the Agency, Activity, and Office structures and between the Agency Basic Cost Accounts, Tasks, and Work Units.
    - Operational Cost – Labor dollar and hour adjustments received from interfacing systems update labor dollar and hour figures in RAS.
    - Military Personnel/Manpower – Maintains current military personnel records and tracks related costs.
    - Performance – Measures work performance and work effectiveness, reporting on how efficiently labor is being used.
    - Online Processing – Access to RAS is through the online, real-time SUPRA database environment.
- AAS
    - Funds Control – Establishes quarterly operating target records as the primary method of controlling available funds.
    - General Ledger Maintenance – Records the receipt of funds, commitments, obligations, expenses, disbursements, and customer orders accepted; and updates the applicable general ledger records online.
    - Appropriation Record Maintenance – Maintains historical records for all transactions that affect the status and utilization of funds.
    - Job Order Accounting – Allows for the establishment of job orders to accumulate costs pertinent to the accomplishment of specific work assignments.

Financial Reporting – Prepares various financial reports and listings to provide data for use by local management and for submission to DFAS-Headquarters, including data utilized for analysis and reconciliation of accounts.

- ABS
    - Reimbursable Receivables – Central point of input and automatic interface of work counts produced in support of Reimbursable Receivables.
    - Funds Control – Controls all work orders, service orders, and work requests received from federal agencies.
    - Excess Earnings – Accounts for the automatic release of suspended excess earnings as additional funds provided by the customer.

System Architecture

DBMS has a two-tiered architecture comprised of:

- Mid-tier and mainframe (hardware and software) components, and
- Remote user/print spooler hardware and software (online viewing, printing, and downloading).

The mid-tier and mainframe components are used as a repository for the collection and accumulation of accounting, billing, labor, and non-labor data. Their primary function is to provide centralized, daily processing of general ledger and cost reports.

The remote user/print spooler hardware and software are used primarily for online report viewing, printing of mainframe-generated outputs, and downloading financial information. These components are largely customer-owned and operated. They include personal computers, local area networks, a diverse assortment of printers, and the software that operates and connects them. Customers have access to "Report.Web" software, which is utilized for viewing, printing, and downloading reports which are produced during nightly batch cycles.

DBMS recently completed a migration where the mid-tier and mainframe servers were moved from DECC-Columbus to SMC-Ogden, as part of the larger DISA transformation strategy currently underway. The DBMS mid-tier server was moved to SMC-Ogden in May 2004, and the mainframe server was moved in February 2005.

ABS is hosted on the mid-tier utilizing an Oracle database. One of its primary functions provides an automatic interface and central point of input for all transactions relating to reimbursable receivable documents. All of the policies guiding the configuration of the database, user account settings, and permissions are controlled by Terminal Area

Security Officers (TASOs). Most of the settings were in place before the box was moved from DECC-Columbus. The Oracle implementation is installed on a mid-tier machine and runs on the UNIX operating system.

The technical components of the DBMS mainframe architecture include the following attributes:

- The hardware supporting the application is housed on the Z890-A-04 mainframe LPAR located at SMC-Ogden;
- The operating system software is z/OS, Release 1.4;
- DBMS is written in COBOL XT, COBOL, and MANTIS 4GL languages;
- The mainframe is initially protected by IBM's Resource Access Control Facility (RACF); and
- Third-party software packages are used for process scheduling and monitoring services.

Both SUPRA LPARs (development and test, and production) transitioned to SMC-Ogden. SUPRA security is implemented through two external security packages: CINCOM ENTIRE controls security at the application level; and RACF controls security at the operating system and dataset levels. The current mainframe operating system for the SUPRA Physical Data Manager database is z/OS, Release 1.4. There are 17 databases, which are configured with the same security settings, passwords and logons.

The two tiers of DBMS architecture are connected via DoD-maintained networks, comprised of Internet Protocol-based (e.g., Non-Classified Internet Protocol Router Network) and Systems Network Architecture-based (leased line) services. These networks connect DBMS to a number of customer sites (mainframes, mid-tiers, and personal computers) that supply or regularly exchange data with DBMS, mainly through electronic file transfers. Examples of some external interface sites include DCPS, SRD-1, and BOSS.

System Interfaces

DBMS customers maintain their own financial management systems that indirectly interface to DBMS in batch cycles via unencrypted FTP. Incoming files from interfacing systems are first processed on a mid-tier platform. The mid-tier utilizes hard-coded logic in the Liaison Activity Code Table (LACT) to route the incoming information to the appropriate DBMS SUPRA database copy. The information is routed if it contains a header and trailer attached by the sending system, signifying the beginning and end of the interfacing file. After the information is routed, it is processed by DBMS and posted to the General Ledger. If information cannot be routed to a

specific database copy,

DBMS sends the specific transaction and logs it to a report on the designated default database for further research by the Accounting Operations Personnel. DFAS-Columbus Accounting Technicians manually corrects the transaction.

Reconciliations are performed by DFAS-Columbus; however, full reliance is placed on the interfacing systems and customers to have rigorous controls in place that catch erroneous information, and missing or duplicate transactions in the batch before transmitting to DBMS.

The most important interfaces include DCPS payroll data, SRD-1 Fund Balance with Treasury information, and BOSS retail stock fund/supply transactions.

The only direct interface to DBMS, bypassing the mid-tier, is a recently-added interface for Defense Commissary Agency – Europe that sends foreign national pay data.

Sensitivity of Data Processed and System Criticality

DBMS contains Sensitive but Unclassified financial information at the Mission Assurance Category (MAC) III level. Actual data elements contain technical, personnel, and financial data that require protection from unauthorized disclosure. The DBMS unclassified environment includes sensitive financial and controlled information that is exempt from mandatory release to the public under the Freedom of Information Act. The DBMS environment includes files, when aggregated/integrated, increases the sensitivity level. To ensure adequate protection of data during FTP processes, DBMS incorporates a Virtual Private Network, when required.

The compromise or unauthorized disclosure of DBMS information would have an adverse impact and actively counter DFAS' mission, functions, image, or reputation. The impact would place DFAS at a significant disadvantage, resulting in intense public scrutiny, loss of public trust, and the possible loss of significant tangible assets or resources. Potential overstatement or understatement of assets, liabilities or net position and significant effects on the completeness and existence of transaction information are possible. DBMS has a recovery window of 72 hours.

Compromise or unauthorized disclosure of DBMS information is prevented through various logical access controls. Specifically, workstations are properly secured to prevent unauthorized access to the application. Users are authenticated with a unique user identification (ID) and password. The application is only available during specified online processing windows corresponding with normal business hours and disconnects after a period of non-usage. Users have three successive failed logon attempts before the account becomes locked and must be unlocked only by a TASO. Finally, access logs are produced that track users logging in and out of the application. A List of Security Violations report tracks failed logins by user and details the reason, usually invalid user passwords or locked accounts.

B. Control Environment

The DFAS-Headquarters, located in Arlington, Virginia, provides management control and coordination within the DoD and has overall responsibility for interpretation and application of DBMS through DFAS-Columbus Accounting Systems Program Management Office.

Administration

Administration of DBMS includes manual operations and standard operating procedures designed to counter fraud, waste, and abuse, including separation of duties, which ensures that work responsibilities are separated so that one individual does not control all critical stages of a process. Physical access to the system will be granted through a rigorous, well-established process conducted in accordance with DoD Directive 5200.2-R, "Personnel Security Program", and Code of Federal Regulations (Chapters 731, 732, and 736).

Personnel

Personnel are assigned security duties to enforce DFAS policies for the operation and protection of DFAS automated information systems. These individuals are knowledgeable in the nature of the information and processes supported by the application and in the management, personnel, operational, and technical controls used to protect the information. The responsibility for implementation, acceptance, and maintenance of adequate automated accounting systems security is assigned to the following individuals:

- The *Program Manager* is responsible for the overall development, delivery, and life cycle maintenance of DBMS and for ensuring that all users have been properly trained and are familiar with security policies and procedures before being granted access.

- The *Designated Approving Authority* is responsible for evaluating the level of risk associated with operating DBMS and granting either an Interim Authority to Operate or an Authority to Operate, if the risk is found to be acceptable.

- The *Information System Security Manager* is responsible for enforcing all applicable security policies and safeguards for all personnel with access to DBMS. In addition, the Information System Security Manager evaluates known or suspected vulnerabilities to ascertain if additional safeguards are needed.

- The *Certification Authority* is responsible for developing and maintaining the accreditation support documentation.

- The *Information System Security Officer (ISSO)* is responsible for day-to-day security administration and security management of DBMS.

- The *TASO* is responsible for performing assigned security tasks as designated by the ISSO, including resetting passwords, suspending or unsuspending accounts, and acting as a general liaison from the user to the ISSO for access-related issues.

C. Monitoring

Management and supervisory personnel at DFAS and DISA monitor the performance quality and internal control environment as a normal part of their activities. DFAS and DISA have implemented a number of management controls that help monitor access to the DBMS application as well as the mainframe. The System Support Office at DFAS-Columbus coordinates access requests and forwards them to SMC-Ogden Security Office to be established in DBMS. Additionally, several application products are in place to monitor systems access to the mainframe LPAR and to the DBMS online portion of the application.

There are performance products on the DISA mainframe to monitor the performance of the hardware and software to ensure the system is performing at maximum efficiency. DFAS and DISA are establishing additional techniques to monitor users' online access to DBMS, including a reading group on the online reporting system which allows Systems area personnel to review, correct, or update online system access.

Violation Listings

DBMS generates violation listings which provide a means of monitoring and correcting the transactions that did not successfully process or interface into DBMS. Transactions attempting to interface into DBMS must meet the established edit, validations, and compatibility criteria before DBMS records and accounts are updated. Transactions that fail to meet these criteria are rejected and appear on violation listings. These violations or rejects all have messages identifying the reason for the rejection.

DBMS also generates violation follow-up listings that contain transactions that have not been cleared by the Accounting Department or the DBMS customer. These violation follow-up listings are generated on a daily basis and transactions remain on the listings with the original error message until corrective action is taken.

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 Designated Approving Authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. 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 information assurance and security posture of the Defense Information Infrastructure. This process supports an infrastructure-centric approach with a focus on the mission, environment, and architecture.

DBMS 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 Designated Approving Authority, the Certifier, user representative, and program manager employed to guide actions, document decisions, specify information assurance requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security. SSAAs were prepared for the DBMS application and the supporting operating environment.

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. DBMS, as well as the business processes it supports, is part of the DoD OIG audit universe and is subject to financial, operational, and information technology (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 DBMS 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. Information and Communication

Information Systems

DBMS is the mixed-function legacy information system serving as the core financial system for several Defense Agencies and the general ledger accounting system of record for those agencies. DBMS indirectly interfaces with a host of financial feeder applications that reside at various DFAS centers, DFAS operating locations, or DISA DECCs through a mid-tier server via unencrypted FTP.

Communication

The support relationship between DFAS and DISA is documented through a SLA, which outlines various DFAS and DISA points of contact and liaisons that should be utilized when issues with DBMS arise.

Within DFAS, the Software Configuration Control Board is responsible for approving and controlling requested functional and systemic changes to DBMS. Through scheduled meetings conducted by the Technical Program Manager, a review of the status of current releases, new change requests, and targeted future release dates is discussed.

E. Control Activities

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

F. User Organization Control Considerations

The control activities at DFAS related to DBMS were designed with the assumption that certain controls would be placed in operation at user organizations. The application of such controls by user organizations is necessary to achieve certain control objectives identified in this report. This section describes some of the controls that should be in operation at user organizations to complement the controls at DFAS and DISA. The following user organization control considerations are not a comprehensive list of all controls that user organizations should employ. Other controls may be required at customer organizations.

User organizations should have policies and procedures in place to provide reasonable assurance that:

- Hard copy documents (e.g., purchase orders, training orders, and miscellaneous obligation documents) are authorized, accurate, and complete before the user enters them into DBMS for input and automated processing.

- Authorized individuals input data into DBMS, enter it accurately and completely, and seek approval from appropriate personnel.

- Erroneous data are corrected and resubmitted in a timely manner.

- The appropriate users review output for completeness and accuracy.

- DBMS computer terminals, communication lines, and data outputs are protected from unauthorized access.

- Passwords needed to access DBMS through computer terminals are protected against unauthorized disclosure and misuse.

- DBMS' TASOs are notified in a timely manner when employees leave or transfer, which supports the TASOs ability to cancel system access authority for those individuals.

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

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

A. Scope Limitations

DFAS and DISA specified the control objectives documented in this section. As described in the prior section (Section II), DBMS interfaces with many systems. The controls and tests described in this section of the report are limited to those computer systems, operations, and processes directly related to DBMS. Controls related to the source and destination systems associated with the DBMS interfaces are specifically excluded from this review. We did not perform procedures to evaluate the effectiveness of the input, processing, and output controls in these interfacing systems, although we did perform procedures to evaluate DBMS' interface input and output controls.

Control Objectives, Control Activities, and Service Auditor's Tests of Operating Effectiveness

Access Control (AC)

Controls provide reasonable assurance that computer resources (data files, application program, system software and computer related facilities, and equipment) are protected against unauthorized modification, disclosure, loss, or impairment.

Control Activity:
AC-1.1 Resource classifications and related criteria have been established.
AC-1.2 Owners have classified resources.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA Security Technical Implementation Guide (STIG) Implementation is at MAC III Sensitive Level. The DISA networks are being protected to MAC III level, while the enclaves are being protected to the highest MAC level operating within the enclave or sub-enclave. The Non-secure Internet Protocol Router Networks are being protected at Sensitive Confidentiality Level. Customers identify the MAC and Confidentiality level for their applications.	**DISA** Inquired security personnel about the criteria used to classify resources. Inspected the DISA Computing Services Security Handbook, DoDI 8500.2, site security plan, and SLA for DISA and DFAS to determine that appropriate resource classifications were established.	**DISA** No relevant exceptions were noted.

Control Activity
AC-2.1: Resource owners have identified authorized users and their access authorized.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA The DISA Computing Services Security Handbook details granting access to system resources. DECC-Columbus users who have access to the mainframe and mid-tier servers where the application resides have completed DD Form 2875.	**DISA** Inspected the DISA Computing Services Security Handbook for the process used to grant access. Inspected the user list and employee list to confirm that all users were on the employee list. Inspected DD Form 2875 for users with access to the mainframe.	**DISA** A list of individuals who can approve access was not maintained for SMC-Ogden. DECC-Columbus: • Did not track privileged role assignments. • Allowed inactive accounts to remain enabled for 180 days before they are reviewed. • Did not disable access for 13 of 45 separated users.

Control Activity:
AC-3.1a: Adequate physical security controls have been implemented. Physical safeguards have been established that are commensurate with the risks of physical damage or access.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA DISA facilities are located on military or General Services Administration installations with controlled access and controlled perimeter. Where Computing Services	**DISA** Toured and inspected the physical layout and environmental controls present in the DECC-Columbus and SMC-Ogden data centers.	**DISA** DECC-Columbus did not have access request forms for individuals to gain physical access to the data center.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
facilities are not located on military or General Services Administration installations, Computing Services facilities are enclosed with a fence that provides vehicle and pedestrian access controls. Local military, DoD, or General Services Administration police perform routine patrol and random door checks. Each site has an agreement with local police organization to perform security checks. In some cases, local police organizations have agreed to perform annual penetration testing; however, not all local police organizations are equipped to perform penetration tests. The computer facility has: • True floor to ceiling walls; • Solid entrance doors; • Doors with hinges that prevent easy removal; • Emergency doors free of devices on the outside and equipped with a panic bar release on the inside and a ½ inch deadbolt throw; • Doors with Balanced Magnetic Switches; • Entrance doors with three-position combination lock for classified areas; and	Inspected that sensitive areas are marked as restricted. Inspected the risk assessment for both DECC-Columbus and SMC-Ogden data centers to determine if threats had been identified. Inspected the process for gaining access to DECC-Columbus and SMC-Ogden data centers. Inquired if management reviewed access to the DECC-Columbus and SMC-Ogden data centers on a periodic basis. Inquired if a facility penetration testing procedure was in place at DECC-Columbus and SMC-Ogden.	DECC-Columbus had not performed a facility penetration test of the data center.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
• Intrusion Detection System for volume within the area for those facilities or areas processing classified information. All intrusion detection system alarms remotely to an external element that can dispatch a response team.		

Control Activity:
AC-3.1b: Adequate physical security controls have been implemented. Visitors are controlled.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA All Computing Services personnel who do not have the appropriate security investigation or clearance will be escorted at all times while in the computing facility. All non-Computing Services personnel will be escorted at all times while in the computing facility.	**DISA** Inspected procedures for handling visitors at the DECC-Columbus and SMC-Ogden data centers. Inquired on procedures to control visitor access to the data centers through a log book. Inspected policies for changing access codes to the data centers' cipher locks.	**DISA** Adequate training was not provided to DECC-Columbus data center personnel to increase their awareness of visitor policies for the data center.

Control Activity:
AC-3.2a: Adequate logical access controls have been implemented. Passwords, tokens, or other devices are used to identify and authenticate users.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA Password configuration requirements: • Minimum of 8 characters, • One lower-case character, • One upper-case character, • One number, and • One special character. Passwords changed every 90 days. Password can only be changed once within 24 hours. Password cannot be reused for 10 cycles. Password cannot reuse any character more than once. Password is individual authentication associated with individual user identification. Passwords are encrypted in storage.	**DISA** Inspected policies and procedures for password parameters. Inquired whether authentication required symmetric keys. Inquired if authentication was accomplished using Public Key Infrastructure Class 3 or 4 certificates. Inquired if concurrent logins was permitted. Inquired how DISA ensured commonly-used names or easily-guessed passwords were not used. Inquired if all contractors were identified by 'CTR' in their e-mail address. Inquired if vendor-supplied passwords were removed from new systems during installation.	**DISA** DECC-Columbus only required three characters to be changed when updating user account passwords.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	Inquired on policies and procedures for control of smart-cards or sophisticated access control devices. Inspected a network diagram that documented logical access points to the Local Area Network	

Control Activity:
AC-3.2c: Adequate logical access controls have been implemented. Logical controls over data files and software programs.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA The mainframe access control application, RACF, protects the DBMS application and the system software it resides on through identification and authentication techniques. RACF mainframe security software enforces discretionary access controls. Also, access to shared and networked file systems outside the mainframe environment is controlled through discretionary access controls enforced through network access privileges. RACF is configured in accordance with the RACF STIG.	**DISA** Inspected the RACF 'SETROPTS' report. Inspected the production 'SETROPTS' report. Inspected production 'DSMON' reports. Inquired if there was a policy requiring every 'applid' to use RACF to validate user IDs and passwords.	**DISA** DECC-Columbus did not comply with STIG for RACF. Testing of the RACF system configuration settings revealed: • Erase-On-Scratch was not active for all sensitive datasets. • Password options such as change interval and history were not set to standard. • No written standard existed to compare which users can have access to SYSTEM SPECIAL, GROUP SPECIAL and SYSTEM AUDITOR. • No standards existed to verify programs in the Program Properties Table with a system key or allowed to bypass RACF validation were appropriate.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
		• Five resource classes were not active and one resource class was active but contained rules that left system unprotected. • The RACF Started Procedures table had duplicate, conflicting entries, and a coding error that made the last part of the table unusable. • Some datasets were listed in the RACF "Selected Datasets Report" as either "not found or not cataloged. • Gaps in procedures for allocation of system datasets, populating them with programs, protecting them with RACF, and marking them Authorized Program Facility (APF)-authorized made it possible for unauthorized APF programs to be added to the system. • RACF rules permitted any user to read or purge any print dataset on the print queue waiting to be printed. • RACF's control of the ability to bypass standard labels on tape datasets was not active. • The RACF Global Access Table permitted every user to have complete access to every dataset whose name begins "SYSOUT."

Control Activity:

AC-3.2d: Adequate logical access controls have been implemented. Logical controls over a database.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
SUPRA System logging should be active to facilitate producing audit reports. The CINCOM vendor recommends that system logging be activated. The system logging options "ABNA" should be used. This will record task sign-on to the database, before-images and after-images of the database records. System logs should be retained to facilitate producing audit reports. Directory files should be properly protected by external security software (e.g. ACF2, RACF, Top Secret). Physical Data Manager system and task log files should be properly protected by external security software (e.g. ACF2, RACF, Top Secret). The SUPRA database files should have appropriate access control. The SUPRA software installation and runtime libraries should have appropriate access control.	**SUPRA** Observed that SUPRA was logging information to two data sets. Inspected the SUPRA logging settings as "ANNA" A- All system sign-ons were logged, N- did not log before images, N- did not log utilities, A-did not log after images. Inquired if SUPRA logs were maintained and how they were used. Inspected the RACF security setting for SUPRA. Inspected the Comprehensive Retrieval Results for five directory files. Inspected RACF for the Physical Data Manager system and task logs. Inspected the RACF security rules for user access to SUPRA datasets. Inspected a list of SUPRA software libraries.	**SUPRA** The "INTERFLM" database had universal access; having read access to certain SUPRA files (INTERFLM in particular) provided a vehicle for updating the databases and should have been limited by user access requirements. Directory files were not protected in the RACF program resource class.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Non-database administrator (DBA) users are allowed into directory maintenance facilities, then directory security should be enabled to control the types of access these users have in the directory. Passwords need to be vigorously protected in job control language input source and in batch job output. Sensitive administrative authorities should be limited to users with a legitimate business need for these authorities (for example, DBA should have the only access to DIRM, etc.). Powerful utilities and functions should be limited to users with legitimate business need for these capabilities (e.g. DBA, security administrator). Stand-alone utilities should be protected by the external security software (e.g. ACF2, RACF, Top Secret). SUPRA security administration functions should be performed by the appropriate personnel.	Inquired about the RACF Customer Information Control System (CICS) access rules. Inspected RACF CICS access rules. Inspected the DBMS Audit MFCP LPAR RACF domain name server Rules and found that the three CICS transactions had read access. Inspected the DBMS MFCP LPAR RACF SUPRA Programs file for security definitions of stand alone utilities. Inquired who performed the security administration for SUPRA.	

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Oracle Database management systems and data dictionary controls have been implemented that: • restrict access to data files at the logical data view, field, or field-value level; • control access to the data dictionary using security profiles and passwords; • maintain audit trails that allow monitoring of changes to the data dictionary; and • provide inquiry and update capabilities from application program functions, interfacing database management systems or data dictionary facilities. Use of database management system utilities is limited. Access and changes to database management system software are controlled. Access to security profiles in the data dictionary and security tables in the database management system is limited.	**Oracle** Inquired of Oracle DBA about the security settings for the Oracle database that supported DBMS. Inspected the Oracle STIG and compared the outputs of the Oracle STIG script to the required settings in the Oracle STIG.	**Oracle** Application user privilege assignment was not reviewed periodically to ensure compliance with least privilege and documented policy. The Oracle version 9.2.0.4.0 was not at the current patchset level, which was version 9.2.0.6. The system tablespace was being used as the default or temporary tablespace for four non-system accounts. Three non-DBA account(s) had been granted Oracle default roles. Access to default replication accounts was not restricted to authorized DBAs. The AUDIT_SYS_OPERATIONS parameter was not set to TRUE. The required minimum of two Oracle control files were not configured and stored on separate physical disks. Database communications was not configured to use static Internet protocol port

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
		assignments to remote database connections. The SQLNET.EXPIRE_TIME had not been set to a value greater than 0 to prevent inactive remote connections to the database. The SQL*Plus HOST command was not restricted to authorized users only. PUBLIC had been granted EXECUTE privileges to restricted. Unauthorized profiles had the password life time set to more than 90 days. The password life time should be set to 90 days or less for user accounts and 365 days for application batch processing accounts. Profiles were found with either PASSWORD_REUSE_MAX not set to 10 or more or PASSWORD_REUSE_TIME not set to 365 or more. The Password Verify Function was not specified. The default profile exceeded the allowed resource limit for Idle Time of 15 minutes.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
		The default profile did not have maximum failed logon attempts set to 3. The SQL92_SECURITY parameter was not set to TRUE. The RENAME object audit option was not specified on default. RENAME was not audited on application objects. The audit trail SYS.AUD$ was not being audited for update and delete by all users. The ORA_ENCRYPT_LOGIN was not set to TRUE to prevent remote login attempts with the password sent in clear text. All required events were not audited in Oracle. The RESOURCE_LIMIT initialization parameter was not set to TRUE.

Control Activity:
AC-4.1: Audit trails are maintained.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA Logging includes: • Minimum unsuccessful attempts are logged to access security files, and logons; • Minimum successful and unsuccessful attempts to modify system controls; and • Records identify user ID, date, and time of event. Audit records are reviewed periodically. Suspected violations are subject to inquiry. Substantiated violations are reported to Information Assurance Manager, who directs required action. Audit records are retained for one year on an external storage device. Audit requirements are listed in each of the STIGs.	**DISA** Inspected the audit trail monitoring, analysis, and reporting processes. Inspected RACF logs. Inquired how long audit records were maintained.	**DISA** System audit records were not maintained for one year.

System Software (SS)

Controls provide reasonable assurance that changes to the existing systems software and implementation of new system software are authorized, tested, approved, properly implemented, and documented.

Control Activity:
SS- 1.1 Access authorizations are appropriately limited.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
OS/390 Policies for restricting access to systems software are detailed in the OS/390. These documents establish guidelines for restricting access to sensitive system datasets. The network device control policy is detailed in the Network Infrastructure STIG, which outlines access restrictions to network devices, and also details the secure configuration of network devices.	**OS/390** Inspected output to determine who had update or greater access to parameter libraries. Inquired on the change control process for parameter libraries. Inquired who reviewed updates made to the production system parameter library. Inspected who had update or greater access to procedure libraries. Inquired what the change control process was for procedure libraries.	**OS/390** DECC-Columbus did not comply with the STIG for OS/390. Testing of the OS/390 operating system configuration revealed: • Three datasets containing user ID and passwords had a default access of READ. • One APF-authorized library could be updated by any RACF-defined user. • Written standards did not specify contents of system libraries. Specifically: o No indication of what user Supervisory Calls had been authorized. o No indication of what APF libraries had been authorized. o No indication of what modifications to the Program Properties Table had been

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
		authorized. • Implementation of changes by DECC-Columbus with no formal and supporting documentation of approval of system software modifications/changes made by DECC-Mechanicsburg.
HP-UNIX Policies and procedures for restricting access to systems software exist and are up-to-date. Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. Application programmers and computer operators are specifically prohibited from accessing system software. The HP-UNIX operating system is configured in accordance with the UNIX STIG.	**HP-UNIX** Inspected the procedures in the Security Features User's Guide for the HP-UNIX platform. Inspected the script results to determine compliance with the UNIX STIG.	**HP-UNIX** FTP and telnet were enabled. Secure Shell was not at the current version. System settings did not in comply with the UNIX STIG.

Control Activity:
SS-2.1 Policies and techniques have been implemented for using and monitoring use of system utilities.
SS-2.2 Inappropriate or unusual activity is investigated and appropriate actions taken.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
OS/390 Mainframe audit log policies are outlined in the OS/390 STIG, Volume 1. The OS/390 STIG requires review of dataset access violations, resource violations, and program use violations on a daily basis and requires review of the failed log-on attempts and security privileges on a weekly/monthly basis. The OS/390 STIG requires the DECC-Columbus to review the RACF global control options at least quarterly to determine whether any changes were authorized and necessary.	**OS/390** Inspected the System Management Facility records selected for logging. Inspected output for key Multiple Virtual Storage system libraries. Inspected output to determine which files were used to collect the system audit trail. Inquired if any user could modify the audit files.	**OS/390** DECC-Columbus did not comply with the STIG for OS/390. Testing of the OS/390 operating system configuration revealed: • Three datasets containing user ID and passwords had a default access of READ. • One APF-authorized library could be updated by any RACF-defined user. • Written standards did not specify contents of system libraries. Specifically: o No indication of what user Supervisory Calls had been authorized. o No indication of what APF libraries had been authorized. o No indication of what modifications to the Program Properties Table had been authorized. • Implementation of changes by DECC-Columbus with no formal and supporting documentation of

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
		approval of system software modifications/changes made by DECC-Mechanicsburg. SMC-Ogden had not implemented effective procedures for monitoring, controlling, and backing-up audit logs recording access to and use of system software and utilities.
HP-UNIX The operating system is configured to prevent circumvention of the security software and application controls and configured in accordance with the UNIX STIG.	**HP-UNIX** Inspected the script results to determine compliance with the UNIX STIG.	**HP-UNIX** No relevant exceptions were noted.

Security Planning (SP)

In order to assess the application controls of DBMS, an understanding of the application's business purpose and financial impact, as well as its processing environment, should be obtained. DFAS should develop a tailored security plan that is in compliance with DITSCAP. DBMS should undergo the certification and accreditation process in accordance with DITSCAP.

Control Activity:
SP-1 Periodically assess risks.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA Periodic evaluations and annual reviews are conducted to determine risk.	**DISA** Inspected risk management policies, DISA Instruction 630-125-6	**DISA** The risk assessment for DECC-Columbus was not performed every three years.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
A formal risk assessment is developed and conducted once every 3 years. Formal risk assessments are updated annually based on annual reviews.	"Management Control Program" and "Residual Risk in DoD" Accreditation issued by FSO. Inspected the risk assessments for DECC-Columbus and SMC-Ogden.	

Control Activity:
SP-1 System documentation for DBMS application exists and is current.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DFAS DBMS technical documentation exists and is current.	**DFAS** Inspected the SSAA for DBMS to determine appropriateness in relation to the current control environment. Inquired of management regarding the current operating environment and current versions of the operating system, database, and security software.	**DFAS** No relevant exceptions were noted.

Control Activity:
SP-2 An application and general support security plan exists and covers the appropriate sections as defined by federal regulations and agency requirements.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA Security plan developed for each site.	**DISA** Inspected the site security plans.	**DISA** Site security plan did not contain Rules of Behavior and OS/390 Security Features User

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DFAS DFAS has documented and finalized a DBMS security plan that contains security policies and procedures (i.e. application security plan, security manuals) containing the following elements of DoDI 8500.2 and National Institute of Standards and Technology Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems": a. Roles and responsibilities of application security officer(s), user managers, users, etc. b. Procedures for granting, modifying, and removing access. c. Standard job profiles. d. Periodic re-certification of user access. e. Monitoring and timely follow-up to access violations and other security-related reports. f. Access only by valid combination of log-on IDs and individual passwords (one unique ID per user). g. Minimum password length (i.e. 8 characters). h. Password character composition (e.g. 1	**DFAS** Inspected the security plan to ensure that updates (if any) were in accordance with DoD and National Institute of Standards and Technology guidance.	Guide. **DFAS** In the DBMS security plan, the appointed personnel to Information Assurance roles were not specified in writing, nor were duties and appointment criteria described.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
numeric, 1 special, 1 symbol, 1 character required). i. Password change period (minimum and maximum number of days). j. Number of password generations. k. Use of encrypted passwords. l. User ID is locked out after a prescribed number of log on failures. m. Deletion of log-on IDs and passwords for separated or reassigned employees. n. Simultaneous use of the same user ID/password is prohibited. o. Menu selections displayed are restricted based upon the access privileges defined by the user ID.		

Control Activity:
SP-2.2 The security plan is kept current.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA Security plan is reviewed annually. Security plan is updated annually or as necessary.	**DISA** Inspected the security plan and the SSAA.	**DISA** DECC-Columbus security plan did not assess changes made to security or the interconnection of systems when changes are made.

Control Activity:
SP-3 Establish a security management structure and clearly assign security responsibilities.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DFAS The DBMS security plan contains the following: a. Effective usage date. b. Name of the person who is responsible for the application. c. Assignment of responsibilities, in writing to ensure that the application has adequate security. d. Description of the following application risk attributes, if applicable: • Connected to the Internet. • Located in a harsh or overseas environment. • Software is rapidly implemented. • Software resides on an open network used by the general public or with overseas access. e. Whether the application is processed at a facility outside of the organization's control. f. Dial-up access support for vendors. g. The security plan contains Rules of Behavior including topics such as, but not limited to:	**DFAS** Inspected the security plan to ensure that updates (if any) were in accordance with DoD and National Institute of Standards and Technology guidance.	**DFAS** In the DBMS security plan, the appointed personnel to Information Assurance roles were not specified in writing, nor were duties and appointment criteria described.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
• Responsibilities of users and user management; • Other policies & procedures unique to the application and its users; • Application rules (i.e. business rules, planned downtime, etc.); and • Dial-in procedures.		

Control Activity:
SP-3.1 A security management structure has been established.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA The DISA Computing Services Security Handbook defines the responsibilities of the Directors, DISA Security Officer, DISA Designated Approval Authority, DISA Certification Authority, Commander of DISA Computing Services Security Manager, DISA Computing Services ISSO, Network Security Officer, and TASO.	**DISA** Inspected the site organization charts, SSAA, and letters of appointment. Inquired about the site security structure from the Information System Security Manager.	**DISA** No relevant exceptions were noted.

Control Activity:
SP- 3.2 Information security responsibilities are clearly assigned.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA The roles and responsibilities of the Information Assurance Manager, Information	**DISA** Inspected the SSAA, security plan, security features user guide, rules of	**DISA** The SMC-Ogden security plan was not complete. Specifically, the plan did not

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Assurance Officer, and Security Manager are outlined in the appointment orders.	behavior, and DISA Computing Services Security Handbook.	sufficiently address all requirements outlined in DoDI 8500.2. Specifically, the security plan: • Did not specify, in writing, the IA roles of appointed personnel nor are their duties and appointment criteria described. • Was not compliant with encryption requirement of Federal Information Processing Standard 140-2, "*Security Requirements for Cryptographic Modules"*, which requires that "unclassified, sensitive data transmitted through a commercial or wireless network be encrypted using NIST-certified cryptography." Though the plan states that mitigation is described in Appendix Q, no Appendix Q was attached to the SSAA. • Did not specify the password minimum or maximum change period. • Did not specify whether menu selections were restricted based on access privileges.

Control Activity:
SP-3.3 Owners and users are aware of security policies.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA DISA Instruction 630-230-19, "Automated Data Processing – Information System Security Program" and the DISA Computing Services Handbook provide guidelines on security training.	**DISA** Inspected security awareness training material for new employees and the annual training material for current employees. Inspected flyers and other means of security awareness communicated to employees. Inspected security training completion sheets and attendance sheets.	**DISA** 35 of 45 employees did not attend new hire security awareness training and three of 45 did not attend annual security awareness training at SMC-Ogden. Eight of 45 employees did not attend annual security awareness training at DECC-Columbus.

Control Activity:
SP-3.4 An incident response capability has been implemented.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA The DISA Computing Services Security Handbook provides guidance on handling incidents, incident reporting structure, and prioritization of incidents.	**DISA** Inquired to personnel about incident response responsibilities. Inspected site SSAA, DISA Computing Services Security Handbook, Network Operations Center Columbus Standard Operating Procedure Incident Response.	**DISA** Incident response process in SMC-Ogden was not specified in the SSAA.

Control Activity:
SP-4 The current processing environment has been authorized by management.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DFAS A C&A has been performed within the last 3 years in accordance with DITSCAP. C&A package contains the following elements: • The Designated Approving Authority and the Security Manager have signed the statement. • Management completed the C&A at the time the application moved into production. • The C&A did not result in an interim authority to operate.	**DFAS** Inquired if a C&A had been performed in accordance with DITSCAP. Inspected the C&A package as part of the DITSCAP process.	**DFAS** No relevant exceptions were noted.

Control Activity:
SP-4.2 Employees have adequate training and expertise.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA Training and Certification requirements for users and system administrators are established by DoD and DISA policies. The DISA Computing Services Security Handbook outlines several different certification courses that system administrators should take depending on the designated level.	**DISA** Inspected job descriptions, personnel records, and education records. Inspected training tracking sheets. Inquired of security personnel about the training and the DISA policy on training.	**DISA** Configuration management staff at SMC-Ogden did not have adequate training. Two of nine individuals did not receive adequate training.

Control Activity:
SP–5.2 Management ensures that corrective actions are effectively implemented.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA DECC-Columbus maintains a plan of action and milestones that tracks all issues identified through a Security Readiness Review including specific weaknesses, resources needed to implement corrective actions, progress in addressing weaknesses, and scheduled completion basis. It is the responsibility of the DECC-Columbus primary security official to send a status to DISA Field Security Office to update their progress on the plan of action and milestones issues	**DISA** Inquired management about the plan of action and milestones process. Inspected the current plan of action and milestones, Corrective Action Plan, and Vulnerabilities Management System.	**DISA** No relevant exceptions were noted.

Change Control (CC)

Effective change controls provide reasonable assurance that DFAS-Columbus has implemented processes to ensure that DBMS software modification responsibilities are carried out in accordance with applicable guidelines. These change control procedures and processes ensure that DBMS processing features and program modifications are properly authorized, new or revised DBMS software is tested and approved, and software libraries are controlled.

Control Activity:
CC-1.1 A System Development Life Cycle methodology (SDLC) has been implemented.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DFAS A SDLC methodology has been developed and approved. The SDLC: • Provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process. • Is sufficiently documented to provide guidance to staff with varying levels of skill and experience. • Provides a means of controlling changes in requirements that occur over the system's life. • Includes documentation requirements. • Program staff and staff involved in developing and testing software have been trained and are familiar with the use of the organization's SDLC methodology.	**DFAS** Inquired of management on DFAS-Columbus responsibilities for change control. Inspected change control procedures in place to ensure responsibilities were carried out in accordance with the SDLC. Inspected any deviations from a standard set of change control procedures. Inquired of staff involved in developing and testing software regarding whether they had been trained and were familiar with the use of the SDLC methodology. Inspected the DBMS configuration management process and software quality assurance controls. Inspected training records to ensure that site personnel had been trained on their change control-related responsibilities.	**DFAS** No relevant exceptions were noted.

Control Activity:
CC-1.2 Authorizations for software modifications are documented and maintained.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA Informational "request" is entered into the Change Control Board Database to keep track of all the changes. Software changes are not made on-site at DECC-Columbus but all modifications are done at Change Design Activities (CDA). As appropriate software becomes available, customers request that DECC-Columbus install the software. For the mid-tier systems, the software is downloaded into a separate directory used only for downloads. After the software is downloaded by CDA, one of the IT Specialists installs the software from that directory into a test directory or system so that the customer can test the program before it goes into production. For the mainframes, the IT Specialists download the software from the appropriate software download site and install it onto a test LPAR.	**DISA** Inspected a sample of changes for appropriate request and development documentation, and approvals.	**DISA** DECC-Columbus did not track software changes through development, testing, and production.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DFAS Software change requests follow a prescribed change control process including: • Documenting all software change requests; • Preparing specification of changes; • Version control of changes; • Conducting unit and process testing; • Completing test plans; • Approval of changes by appropriate manager; and • Coordinating implementation with the System Owner.	**DFAS** Obtained and inspected a list of recent software modifications (regular and emergency changes). For a sample of changes, inspected documentation to determine whether the following requirements were met: • DFAS completed application change request forms; • Appropriate management authorized these forms; • Each change request form had a unique identification number; • Change specifications were clearly documented; • A configuration management plan existed; • Documented test plans and results existed to support the change; • DFAS documented and analyzed test failures to detect ineffective testing; • Changes were moved into production following management's approval; and • DFAS documented user acceptance.	**DFAS** 18 of 19 mid-tier change releases were missing either the ATQ [1] signature or the Program Management Office signature block. Three of five major/minor release test plans provided did not have results documented.

[1] ATQ is an office code within DFAS-Columbus. This is not an acronym.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	Inquired as to the frequency of Configuration Control Board meetings for changes affecting the site.	

Control Activity:

CC-2.1 Changes are controlled as programs progress through testing to final approval.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DISA Informational "request" is entered into the Change Control Board Database to keep track of all the changes. Software changes are not made on-site at DECC-Columbus but all modifications are done at CDA. As appropriate software becomes available, customers request that DECC-Columbus install the software. For the mid-tier systems, the software is downloaded into a separate directory used only for downloads. After the software is downloaded by CDA, one of the IT Specialists installs the software from that directory into a test directory or system so that the customer can test the program before it goes into production. For the mainframes, the IT Specialists	**DISA** Inspected the sample of changes for test plans.	**DISA** DECC-Columbus did not track software changes through development, testing, and production.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
download the software from the appropriate software download site and install it into a test LPAR. **DFAS** Changes to DBMS are logged to provide "trace-back" ability. At each level of testing, there is management approval before proceeding to the next level of testing. Evidence of management is maintained. An independent group, such as Quality Assurance, moves changes between development, testing, and production environments. Security requirements are considered and approved. These security features are tested for emergency changes. Supporting documentation for system administrator, operators, and end-users were updated after changes/modifications to the selected sample systems.	**DFAS** Inquired whether changes to applications were logged to provide "trace-back" ability. Inspected supporting documentation for five last major changes. Inquired as to whether at each level of testing, there was management approval before proceeding to the next level of testing. Inquired as to what type of data was used during the testing of changes made to DBMS. Also, observed who reviewed and accepted test results. Inquired as to who was responsible for moving changes between development, testing, and production environments. Inquired if supporting documentation for system administrator, operators, and end-users was updated after changes/modifications to the selected sample systems.	**DFAS** No relevant exceptions were noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	Inspected Release letters with functional documentation.	

Control Activity:
CC-2.2 Emergency changes are promptly tested and approved.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Finalized policies and procedures are in place for emergency changes. These documents require emergency changes to be recorded and approved by management; and normal change request forms and documentation are to be completed after the emergency change.	Inspected policies and procedures in place for emergency changes to determine if emergency changes were recorded and approved by management; and normal change request forms and documentation were completed after the emergency change.	16 of 45 emergency change releases did not have documentation to support the changes. Two of 29 emergency change releases did not have the appropriate signatures on the Technical Management Certification Release Quality Certification Checklists. One of 29 emergency releases was missing the appropriate signature on Release Quality Certification Checklist Product Integration Certification. Six of 29 emergency change releases and 19 of 19 mid-tier releases did not have a Technical Management Verification signature on the TCA/CO[2] Transmittal Forms.

[2] TCA/CO is an office code with DFAS-Columbus. This is not an acronym.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
		26 of 29 emergency change releases were missing either the ATQ signature or the Program Management Office signature block on the Quality Certification Checklist.

Control Activity:
CC-3.1 Programs are labeled and inventoried.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Finalized policies and procedures exist for the labeling and inventorying of DBMS programs. DFAS-Columbus uses automated software libraries to record the movement of software applications. DFAS-Columbus maintains the following: • An audit trail of program changes; • Current program version numbers; • The location of prior versions; and • Location and status of physical media.	Inspected policies and procedures for the labeling and inventorying of software programs. Inquired if DFAS-Columbus used automated software libraries that record the movement of software applications. Inspected a listing of the programs maintained in each library.	No relevant exceptions were noted.

Control Activity:
CC-3.2 Access to program libraries is restricted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DFAS-Columbus has established separate	Inquired if DFAS-Columbus had separate	No recertification policy or process was in

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
environments for development, testing, and production. DFAS-Columbus restricts the unauthorized access and/or modification of source code via RACF/Endeavor. Programmers/developers do not have access to the production environment, and end users do not have access to the development and test environments. The development environment is certified and accredited. The source code for the most recent DBMS version is maintained in a separate library from production code. DFAS maintains backup tapes/media for production library.	environments for development, testing, and production. Inquired how access was controlled between these environments (development, test, and production) for non-end users. Inspected a listing of non-end users with access to development and test, and production environments. Inquired if source code for the most recent version of DBMS was maintained in a separate library from production code. Inspected a listing/inventory of program tapes/media. Inspected the existence of a sample of ten program tapes/media either in the library or with the individual responsible for withdrawing the tapes/media.	place to ensure that user access and privileges in DBMS were appropriate.

Control Activity:
CC-3.3 Movement of programs and data among libraries is controlled.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Finalized policies and procedures exist for movement of program code between	Inspected policies and procedures for movement of program code between	No relevant exceptions were noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
libraries. The movement of changes are approved and documented by responsible management.	libraries. Inquired if movement of changes were documented and approved. Inspected recent changes and screen prints of the changes.	

Authorization (AN)

Only authorized transactions should be entered into DBMS and processed by the computer. Assessing authorization controls involves evaluating the entity's ability to effectively perform the following critical elements:

- All data are authorized before entering DBMS.
- Data entry terminals are restricted to authorized users for authorized purposes.
- Master files and exception reporting help ensure all data processed are authorized.

Control Activity:
AN-1.1 Source documents are controlled and require authorizing signatures.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Input transactions received are entered either by interfaces from another system or are input manually by Accounting Technicians. All transactions are assigned unique function code prefixes to identify source.	Inspected the applicable standard operating procedures for entering transactions into DBMS. Obtained and inspected a listing of function code prefixes. Obtained and inspected examples of source	No relevant exceptions were noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Key source documents require authorizing (at least one of the following) signatures (Supervisor, Contract Officer, Resource Manager, Billing Official) for: • 1081 – Accounting adjustment document; • Modification of Documentation – Used to modify an existing contract; • Military Interdepartmental Purchase Requests – Used for procurement of commercial supplies and/or services; and • Contracts – Binding documents with outside vendors. Manual source documents are controlled with a block number assigned by DDARS. Block numbers are used to maintain sequence control and accountability over the documents. Vouchers within the block are totaled on the block by appropriation code. Accounting Operations is responsible for verifying all manual input documents	documents used to enter each class of obligations, which includes: a. Commitments, b. Obligations, c. Work Counts, d. Expenses, e. Disbursements, f. Payables, g. Receivables, and h. Journal vouchers. Observed Accounting Operations staff perform their job functions and process block tickets for different transactions. Inquired where original source documentation was stored. Inspected prepared source documents and batches. Inspected procedures for recording and tracking pre-numbered documents.	

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
through control totals and identification of user ID of technician who was responsible for the input.		

Control Activity:
AN-1.2: Supervisory or independent reviews of data occur before data enter the application.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Data control unit personnel verify that source documents are properly prepared and authorized. Data control unit personnel monitor data entry and processing of source documents.	Inspected standard operating procedures for entering data into DBMS. Inquired on security controls in place to prevent unauthorized users from entering fraudulent transactions. Inquired if supervisory review of transactions takes place through signed document, email, or other means. Observed the Block Ticket process. Inspected Block Ticket transactions.	No relevant exceptions were noted.

Control Activity:
AN-2.1 Data entry terminals are secured and restricted to authorized users.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DD Form 2875 must be completed by individual requesting access with required supervisor signature. An additional program	Inquired to the ISSO about the procedures in place to obtain a DBMS user ID.	Inadequate security settings were in place to ensure that DFAS-Columbus computer users were automatically logged out of their

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
worksheet annotating which accesses is required and must be submitted with the DD Form 2875, which requires supervisor signature. The DD Form 2875 is sent to the security manager to validate the background investigation or clearance information. For external users only, a supervisor signature and security clearance from their location is required, prior to submission to DFAS-Columbus. Additional program worksheet annotating which access levels are required must be submitted with the DD Form 2875. The worksheet requires supervisor signature. For certain access levels, some menus requests require the Division Chief's signature. DECC-Columbus would assign the program access. The TASOs would assign the Activity access and notify the user of their user ID and temporary password. Data entry is accomplished through a password protected (CAC) terminals which are located on the users' desks.	Inquired about additional logical access controls in place to restrict access to user terminals. Inquired and observed how workstations were secured to prevent unauthorized access. Inquired and observed how DBMS users access the application. Inquired if a supervisor was required to approve the logon for each session. Inquired if each user was required to use a different user ID. Observed and inspected the password settings used for DBMS. Inspected the DBMS environment password configurations to determine if they were set to the following parameters: • Be at least eight characters; • Include at least one upper case, one lower case, number, and one special character; • Require that at least four characters be changed when creating a new password; • Force default/factory setting passwords	terminals after a specified period of inactivity. In addition, computer terminals were left unattended with CACs inserted and screen lock not activated. DBMS password settings, controlled by ENTIRE, were not compliant with DoDI 8500.2. None of the password settings, for either the TSO or the DBMS application, could be verified by viewing the actual CINCOM ENTIRE program logic. The following ENTIRE settings were not in compliance with DoDI 8500.2: • Passwords with at least one alphabet, numeric, and special character. Passwords are not case sensitive. • New password with three changed characters. • Password encryption (DFAS-Columbus can not prove that passwords are properly encrypted). Six users who were listed as separated still had active DBMS user accounts. DFAS-Columbus procedures and processes over DBMS user account management did not comply with the DFAS-Columbus Handbook

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
When a terminal is not in use, the terminal CAC is removed and the terminal is locked. The system requires a CAC, as well as user ID and password, for re-entry into the network. A separate/unique user ID and password is required to log-on to DBMS. DBMS is programmed to allow data entry connections (i.e., "sign-on") during specified periods of the day that correspond with the online hours of the system. Data entry connections automatically disconnects from the system after 15 minutes of inactivity. Internal users are required to sign acknowledgement forms stating their responsibility for their account ID and temporary password. Sign-on requires users to establish passwords known only to them. All transactions are logged as entered, along with the ID of the person entering the data.	to be removed/changed upon initial use; • Contain system mechanisms to force automatic expiration of passwords and prevent password reuse; and • Require password files to be encrypted. Inquired if users could access the application directly or if they needed to logon to the local area network or mainframe first. Inspected the DBMS user list, current employee list and terminated employee list. Inspected 209 access request forms. Inquired on re-certification of user and programmer access. Inquired if users were locked from accessing the application during specific periods. Inspected the output of attempting to logon to a workstation outside of the permitted window. Inquired if users were disconnected after a specific period of inactivity. Inquired if successive logon attempts were	for Systems Access Management and Control and DoDI 8500.2. The following control weaknesses were identified: • 171 of 209 users did not have DD Form 2875 on file at DFAS-Columbus. Only 13 of the 38 who did have files maintained had their access request form, DD Form 2875s, correctly filled out, and only 20 had access request worksheets, specifying the function codes. The remaining 25 access request forms and 17 access request worksheets were either incomplete, missing DBMS TASO signatures, or did not have appropriate justification. • No recertification policy or process was in place to ensure that user access and privileges in DBMS were appropriate. DFAS-Columbus management had no way of knowing when external users no longer needed access unless their supervisors informed the DBMS TASOs. Furthermore, DFAS-Columbus management did not periodically review application programmer privileges access and privileges. DFAS-Columbus did not have procedures and

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	controlled and monitored. Inquired if users could access the application via dial-up. Inquired what types of users had dial-up access and if the transmission was encrypted. Inquired what controls were established for dial-up. Inquired if access logs were maintained by DBMS. Inquired on and inspected procedures for review of the access logs. Inspected example of DBMS access logs.	processes in place to review the access logs for DBMS for either unauthorized accounts or inappropriate user activity. No previous log reviews existed to verify that access logs were properly created and periodically monitored.

Control Activity:
AN-2.2: Users are limited in what transactions they can enter.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Security is exercised by the system at levels in the processing cycle through the system sign-on, menu selections/authorization, and activity identity. User access is restricted by the user-assigned functions and password. This	Inquired if DBMS had authorization profiles for the application and SUPRA. Inquired to DBMS management if the access matrix in the SSAA was followed. Inspected the adequacy of the general controls over authorization profiles.	DFAS-Columbus procedures and processes over DBMS user account management did not comply with the DFAS-Columbus Center Handbook for Systems Access Management and Control and DoDI 8500.2. Specifically: • Position descriptions could only be

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
security is authenticated through SUPRA. SUPRA applies security to activities that have the accounting function completed at DFAS. The user must be authorized to sign on to DBMS. Subsequent access will be determined by management and implemented by the Automated Data Processing Field Security Representative. Authorization will link the user to either Appropriation Accounting Programs or a subsequent menu which authorizes access to only a limited number of function codes within DBMS. Access is based on assigned tasks, not job descriptions. Sign-on requires the user to establish a password known only to the user which will further restrict access.	Inspected the listing of the DBMS profiles and their description. Inquired and inspected the types of activities authorization profiles were used to control. Inspected 209 access request forms. Inquired and inspected that authorization profiles limited the dollar amount of a transaction a user could enter, edit, or approve. Inspected documentation to determine whether access to menus/screens corresponds to the users' defined duties. Inspected 209 access forms and compared them to the UTYS02 (user list) report to determine that users had access to what was approved.	provided for 15 of 38 users. Of these 15, one did not justify needing access to DBMS. • There was no process in place to verify that supervisors properly assigned function codes to promote segregation of duties. • Nine of 37 users had access request worksheets that correctly matched the user's actual access in DBMS.

Control Activity:
AN-3.1: Master files help identify unauthorized transaction.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Before transactions are processed, they are verified using master files of approved	Inspected documentation on validity and accuracy checks performed on data fields.	No relevant exceptions were noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
lines of accounting as appropriate for the application. Master files consist of: • LACT (a program file), • Master Accounting Data, and • Matrix. Master file LACT that does the verification is protected from unauthorized modifications.	Inquired from the DBMS programmers how data was verified and what type of information was verified before the transaction was processed. Inquired how master files that contained vendor, customer, or other sensitive information were secured. Inquired who had access to master files. Inquired how access was granted and whether it was noted on access request form. Inspected and observed a sample of function codes for the tables, confirming that transactions verify information in the tables or files properly.	

Control Activity:
AN-3.2: Exceptions are reported to management for their review and approval.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
General ledger account code adjustments, based on parameters established by the standard operating procedure Journal Vouchers Adjustments to the General Ledger, are tracked on a monthly report for management review and approval.	Inquired if DBMS produced a violation file of rejected information (hard or soft formats). Inspected violation reports for the past six months for receivables-reimbursable and	No relevant exceptions were noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	non-reimbursable, SRD-1, and BOSS violation control listing, and BOSS invalid transaction journal. Inquired if there were criteria for exception/rejection reporting. Inspected documentation establishing reporting parameters for exception/rejection reporting.	

Completeness (CP)

All authorized transactions should be entered into and completely processed by the computer. Assessing the controls over completeness involves evaluating the DEFAS-Columbus' ability to effectively:

- Ensure all authorize transactions are entered into and processed by the computer.
- Ensure reconciliations are performed to verify data completeness.

Control Activity:
CP-1.1 Record counts and control totals.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DDARS generated block tickets provide established counts and control totals over source documents, utilizing the Disbursing Daily Cash Blotter to help determine the completeness of the data entry and data processing.	Inspected documented procedures for using record counts and control totals when entering transactions. Inquired how record counts were generated. Obtained and inspected output of the counts developed.	No relevant exceptions were noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Online or real-time system and control totals per appropriation are reflected on each control block (daily) and are used to help determine the completeness of data entry and processing.	Inquired how the accumulation of record counts were used, and how they were recorded (each session, daily or other frequently).	

Control Activity:
CP-1.2 Computer sequence checking.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Sequence checking is used to identify missing or duplicate transactions through auto-marking in DDARS. Reports of missing or duplicate transactions are produced from DDARS. Exceptions are investigated and resolved by month-end.	Inquired if serial numbers from source documents were used for sequence checking. Inquired if a sequence checking review was performed to check for duplicate or missing transactions. Obtained and inspected examples of the sequence checking reports. Inquired what actions were taken for duplicate or missing documents.	No relevant exceptions were noted.

Control Activity:
CP-1.3 Computer matching of transaction data.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Computer matching of transaction data with data in master or suspense files occurs to identify missing or duplicate files.	Inquired if unique identifiers were assigned to each transaction. Inquired if DBMS performed automated	No relevant exceptions were noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
DDARS reports of missing or duplicate files are produced and items are investigated and resolved by month-end.	checks of transactions to identify missing or duplicate transactions. Inspected policies and procedures to determine how missing or duplicate transactions were reported and investigated. Inspected how missing or duplicate transactions were investigated and resolved.	

Control Activity:
CP-1.4 Checking reports for transaction data.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Individual transactions or source documents are compared through DDARS auto-marking, with a detail listing of items processed by the computer, particularly to control important low-volume, high-value transactions.	Inquired if users (internal and external) of DBMS compared source documentation to reports produced by DBMS to verify information is accurate. Inquired if transactions considered low volume, but high dollar value were reviewed separately with source documentation. Inspected the procedures regarding source documentation. Observed Accounting Technicians performing their job functions for the purpose of inspecting source documentation.	No relevant exceptions were noted.

Control Activity:
CP-2.1 Reconciliations show the completeness of data processed at points in the processing cycle.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Record counts and control totals are established by block totals and reconciled with transaction data manually and through DDARS auto-marking. Trailer labels or control records containing record counts and/or control totals are generated for batch interface files and tested by DBMS (part of the program logic) to determine that all records have been received. Reconciliations are performed to determine the completeness of transactions processed and whether master files updated and outputs generated: • Daily, • As-Required, • Monthly, • Using DDARS, and • Using Automated Trial Balance Reconciliation.	Inquired how management ensured that all transactions were complete once they were entered into DBMS. Inspected related policies and procedures.	Although DFAS represented that a header and trailer were required for all files sent from interfacing systems, DBMS accepted files in its entirety without the trailer and allowed the information to post to the system. In addition, inbound interface between DBMS and SRD-1 is not operating correctly when information is sent to DBMS. Specifically: • DBMS will accept data files from SRD-1 when trailer records are not included in the transmission. • DBMS does not notify DFAS-Columbus management that trailer records were not received.

Control Activity:
CP-2.2 Reconciliations show the completeness of data processed for the total cycle.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Trailer labels or control records containing record counts and/or control totals are generated for batch interface files and tested by DBMS (part of the program logic) to determine that all records have been received. Reconciliations are performed to determine the completeness of transactions processed, master files updated, and outputs generated: • Daily, • As-Required, • Monthly, • Using DDARS, and • Using Automated Trial Balance Reconciliation.	Inquired how management reconciled transaction information. Inspected the reports to re-perform a sample of 45 reconciliations over the past six months to determine procedures were followed. Inquired on interface controls for major interfacing system. Inquired how DBMS reconciled the in-bound and out-bound interfaces. Obtained and inspected a sample of reconciliation reports. Inquired if the customers of DFAS were responsible for completeness of the interface transactions.	The interfaces to and from DBMS were not encrypted. Sensitive financial data was transmitted over the interfaces in clear text via unsecured FTP. Although headers and trailers were required for all files being sent from interfacing systems, DBMS accepted the files in its entirety without the trailer and allowed the information to post. The inbound interface between DBMS and SRD-1 was not operating correctly when information was sent to DBMS. Specifically, DBMS accepted data files from SRD-1 when trailer records were not included in the transmission. DBMS did not generate a violation report when trailer records were not received.

Accuracy (AY)

The recording of valid and accurate data into an application system is essential to provide for an effective system that produces reliable results. Assessing the controls for valid and accurate data involves evaluating DFAS-Columbus' ability to effectively ensure:

- Data entry design features contribute to data accuracy.
- Data validation and editing are performed to identify erroneous data.
- Erroneous data are captured, reported, investigated, and corrected.
- Review of output reports helps maintain data accuracy and validity.

Control Activity:
AY-1.1 Source documents are designed to minimize errors.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
The source document is well-designed to aid the preparer and facilitate data entry.	Inquired that source documents had been effectively designed to aid in the data entry of transaction information. Obtained and inspected blank source documents to confirm that they aided the preparer to record data correctly and in a uniform format. Inspected the master list of function codes. Inquired if the function codes used for data entry into DBMS were entered on source documentation. Inspected sample source documentation.	No relevant exceptions were noted.

Control Activity:
AY-1.2 Pre-formatted computer terminal screens guide data entry.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Pre-formatted computer terminal screens are utilized and allow prompting of data to be entered, and editing of data as it is entered.	Inquired and observed that screens were pre-formatted for data entry. Inquired and observed that screens prompted the user to enter data by field.	No relevant exceptions were noted.

Control Activity:
AY-1.3 Key verification increases the accuracy of significant data fields.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Mandatory fields for edits and validation to ensure key data is entered. Online editing is performed to prevent erroneous data from being keyed. Invalid changes to key data elements are not permitted.	Inquired and observed that DBMS did not require data fields to be re-enter to verify data accuracy before it was accepted. Observed Accounting Technicians entering data to ensure all data fields were entered before the transaction was processed.	No relevant exceptions were noted.

Control Activity:
AY-2.1 Programmed validation and edit checks identify erroneous data.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
All transactions are subject to validations and edits, which include checks for: • Accuracy – Negative Unliquidated Obligation Edits, • Dependency, • Existence, • Mathematical accuracy, • Check digit – Numeric not alpha, • Document reconciliation, and • Relationship or prior data matching. Validation and editing are performed at the computer terminal during data entry or are performed as early as possible in the data flow and before updating master files. All applicable data fields are checked for errors before rejecting a transaction.	Inquired from DBMS programmers how DBMS ensured that "correct data type" was entered into the field (i.e. alpha, numeric). Inquired what controls were in place to ensure completeness and accuracy of input (reconciliation of control totals, 1-for-1 checking, matching, sequence checking, duplicate processing, and programmed edit checks). Inquired if and how the following automated edit checks were performed on the input data: • Reasonableness, • Limit Check, • Range, • Existence, • Format, • Check Digit, • Duplicate Check, and • Completeness Check. Inquired whether the following edit checks existed:	The means for which DBMS ensured that correct data type (i.e. alpha or numeric) was entered into a data field could not be verified.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	• Format checks on numeric data; • Range checks on variable numeric field; • Date tests on date fields; • Existence checks on all key fields; • Check digit on all identification keys; • Tests for missing data; • Tests for extraneous data; • Tests for record mismatches; and • Tests for out of sequence conditions. Inspected each edit check being performed in the system. Inquired how data received from interfacing applications were validated for completeness and accuracy. Inspected interface transactions files for edit checks.	

Control Activity:
AY-2.2 Tests are made of critical calculations.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Program code and criteria for tests of critical calculations are protected from unauthorized modifications. All calculations are tested in the Change Control Environment.	Inquired on DFAS-Columbus' responsibilities for change control, including the following:	No relevant exceptions were noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Manual controls depend on Accounting Operations verifying the daily & monthly data.	• Application modifications (enterprise and business applications); • Testing and approving software changes; • Quality assurance or quality control; • Controlling software libraries; and • Migrating changes to production. Inspected DBMS configuration management procedures. Inquired whether each level of testing had management approval before proceeding to the next level of testing. Inquired how management ensured that all transactions were complete once they were entered into DBMS. Obtained and inspected related policies and procedures. Obtained and inspected any output or reports. Inquired how management reconciled transactions information. Obtained and inspected applicable output or reports. Inspected the reports to re-perform a sample of reconciliations over the past six months to determine procedures were followed.	

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	Inquired on the fields required for any transaction to be processed to the next level. Inquired whether DBMS had built-in logic to allow for "auto-complete". Inquired on the change control process for updating an "auto-complete" list/menu.	

Control Activity:
AY-2.3 Overriding or bypassing data validation and editing is restricted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Overriding and bypassing data validation and editing are restricted.	Inquired if users were able to override information when entering transactions and who had this capability. Inquired if DBMS produced a report listing for: • Transactions and data elements that were overridden; and • User IDs with the ability to override transactions and data elements.	No relevant exceptions were noted.

Control Activity:
AY-3.1 Rejected transactions are controlled with an automated error suspense file.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Interface-rejected data are automatically written on an automated violation file and held from processing until corrected. Each erroneous transaction is annotated with: • Error messages indicating the type of data error; • Date and time the transaction was processed and the error identified; and • The identity of the user who originated the transaction. The suspense file is purged of transactions as they are corrected.	Inquired if audit trails tracking transactions and user activity were maintained. Inspected the most recent audit trail. Inspected policies and procedures for performing periodic review of the audit trail for unusual activity. Inspected the most recent audit trail review. Inquired whether the contents of audit trails were protected against unauthorized access, modification, and deletion. Inquired how long audit logs were retained. Inquired if transactions that were rejected were sent to a suspense file and held until they were investigated and corrected. Inspected the most recent suspense file. Inquired who reviewed the suspense file and investigated and cleared the items. Obtained and inspected policies and procedures for reviewing, investigating and correcting items in the suspense file.	DFAS-Columbus and SMC-Ogden did not conduct periodic reviews of the DBMS audit trail for unusual activity. DFAS-Columbus did not have policies and procedures in place for the review, investigation, and correction of rejected transactions located within the violation file. As a compensating control, there were overviews and an appendix covering error codes and clearing violations in AAS and ABS that is distributed to all associates who enroll and complete training classes. The identity of the user or original rejected transaction was not identified in the violation file. As a compensating control, the identity of the user or originated transaction was located on the block ticket. Unable to verify that all sample rejected transactions were corrected since all documentation requested from the violation file sample was not provided.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	Inspected items in the suspense file from the six months and reviewed how they were resolved.	

Control Activity:

AY-3.2 Erroneous data are reported back to the user department for investigation and correction.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Accounting Operations is responsible for monitoring and correcting rejected transactions. A report is generated on a daily basis that identifies all open violations for management review. Errors are corrected by the Accounting Technician assigned to support that customer. Function Codes control access to the suspense file.	Inquired how rejected transactions were reported. Inquired who corrected the rejected transactions. Inquired whether supervisors reviewed corrected transactions. Inspected supporting documentation for a sample of rejected and corrected transactions over the last six months.	No relevant exceptions were noted.

Control Activity:
AY-4.1 Control output production and distribution

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
The DBMS System Division is responsibility for ensuring that all outputs are produced and distributed according to customer requirements. The data processing control group, or some alternative: • Has a schedule by application that shows when outputs should be completed and passed to OLRV. • Reconciles control information to determine completeness of processing. The Mechanization of Reports Distribution System automatically checks the output message before displaying, writing, or printing to make sure the output has not reached the wrong terminal device. Output from reruns is subjected to the same quality review as the original output.	Inquired which division/department was responsible for ensuring that all outputs (reports) were produced and distributed according to the requirements of DBMS and user management. Inquired whether the data processing control group maintained a schedule, by application, that showed: • Output products produced; • When they should have been completed; • Who the recipients were; • The copies needed; and • When they were to be distributed. Inquired if a schedule had been established for month-end, quarter-end, and year-end report processing. Inspected a copy of this schedule.	No relevant exceptions were noted.

Control Activity:
AY-4.2 Reports showing the results of processing are reviewed by users.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Output reports for data accuracy, validity, and completeness are reviewed by multiple end users (Management, Accountants, Technicians, etc.) based on the nature of data being reviewed, including: • Error reports, • Transaction reports, • Master record change reports, and • Control totals balance reports. Printed reports contain a title page with report, name, time and date of production, the processing period cover; and have an "end-of-report" message.	Obtained and inspected examples of the reports produced by DBMS. Compared the reports to information in DBMS for completeness. Inquired that each report had a title page with the name, time and date of production, and had an end-of-report page. Observed and inspected these reports. Inquire if a log was maintained for all reports produced. Inspected the log for printed reports. Inquired that the contents of reports were protected against unauthorized access, modification, and deletion. Inquired if any reports were sent to supervisors to approve prior to issuance. Inspected a sample of reports that were approved. Inquired if a log of output errors was	Error, transaction, and master record change reports from the OLRV did not include an end-of-report page.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	maintained. Inspected the log of output errors. Inquired if users reviewed reports for data accuracy, validity, and completeness.	

Integrity (IN)

Controls provide reasonable assurance that production processing uses the current version of software and data, that programs include routines for checking internal file header labels before processing, and that concurrent updates of files are not allowed.

Control Activity:
IN-1 Integrity controls over processing and data files ensure the current version of production is used during processing.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Procedures ensure that the current versions of production programs and data files are used during processing by completing Release Check Lists. Programs include routines for checking internal file header labels before processing. The application protects against concurrent file updates.	Inspected policies and procedures that ensure that the current version of production programs and data files was used during processing. Inquired that DBMS included routines to verify that the proper version of the computer file was used during processing. Inquired that DBMS included routines for checking internal file header labels before processing. Inquired that DBMS protected against	No relevant exceptions were noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	current file updates. Inquired that DBMS used transaction roll-back and transaction journaling. Inquired that DBMS management maintained a current baseline inventory of all software required to support system operations.	

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

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

Continuity of Operations Planning

Based on the SLA between DECC-Columbus and DFAS-Columbus Accounting Services, DECC-Columbus agreed to provide COOP services to DFAS-Columbus. Specifically, DECC-Columbus agreed to:

- Support and maintain back-up tapes.
- Ensure off-site storage back-ups are performed weekly. These procedures are in place to validate the integrity of back-up tapes prior to being sent off-site.
- Perform off-site storage back-ups as required by DFAS-Columbus, which has classified DBMS as 'critical' and is to be recovered immediately at an alternate processing site.

The COOP Assessment in the SSAA for DBMS that was dated January 1, 2003, contained the following table summarizing DBMS' contingency readiness:

CONTINGENCY PLAN EVALUATION	YES	NO	N/A
Is there a contingency plan in existence for this system?	X		
Does the contingence plan, at a minimum, address the following:			
The actions required minimizing the impact of a fire, flood, civil disorder, natural disaster, or bomb threat	X		
Backup procedures to conduct essential IS operational tasks after a disruption to the primary IS facility	X		
Recovery procedures to permit rapid restoration of the IS facility following physical destruction, major damage or loss of data	X		
Does this contingency plan provide for the following:			
Storage of system back-up data in off site storage or in the central computer facility in metal or other fire retardant cabinets	X		
Duplicate system tapes, startup tapes/decks, database save tapes, and application program tapes unique to the site to be maintained in a secure location removed from the central computer facility	X		
Identification of an alternate site containing compatible equipment	X		
Destruction or safeguarding of classified material in the central computer facility in the event that the facility must be evacuated	X		
The contingency plan has been tested during the past year	X		
The ISSO maintains a copy of the contingency plan	X		
The contingency plan contains criteria to state when it should be implemented and who can make that decision	X		

Acronyms and Abbreviations

AAS	Appropriation Accounting Subsystem
ABS	Automated Billing System
APF	Authorized Program Facility
BOSS	Base Operations Support System
C&A	Certification and Accreditation
CAC	Common Access Card
CDA	Change Design Activities
CICS	Customer Information Control System
DBA	Database Administrator
DBMS	Defense Business Management System
DCPS	Defense Civilian Pay System
DDARS	Distributed Data Archive and Retrieval System
DD Form 2875	System Authorization Access Request
DECC	Defense Enterprise Computing Center
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DITSCAP	Defense Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DoDI	Department of Defense Instruction
FTP	File Transfer Protocol
ID	Identification
IT	Information Technology
ISSO	Information System Security Officer
LACT	Liaison Activity Code Table
LPAR	Logical Partition
MAC	Mission Assurance Category
OIG	Office of the Inspector General
OLRV	Online Report Viewer
RACF	Remote Access Control Facility
RAS	Resource Administration Subsystem
SDLC	System Development Life Cycle
SLA	Service Level Agreement
SMC	Security Management Center
SRD-1	Standard Financial System Redesign Subsystem
SSAA	System Security Authorization Agreement
STIG	Security Technical Implementation Guide
TASO	Terminal Area Security Officer
TSO	Time Sharing Option
z/OS 1.4	z/OS, Release 4, Version 1.4

Report Distribution

Office of the Secretary of Defense

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

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Combatant Command

Inspector General, U.S. Joint Forces Command

Other Defense Organizations

Director, Defense Finance and Accounting Service – Accounting Services
Director, Security Management Center - Ogden

Non-Defense Federal Organizations

Government Accountability Office
Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
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 the Inspector General produced this report.

Paul J. Granetto
Patricia A. Marsh
Addie M. Beima
Michael Perkins
Kenneth H. Stavenjord
Donna A. Roberts
LTC Shurman Vines
Cindy Gladden
Ahn Tran
Towanda L. Stewart
Anissa M. Nash
Patricia A. Joyner
J. Shawn Sparks
Brian A. Royer