

October 24, 2005



Information Technology Management

Report on Defense Departmental
Reporting System and Related
Financial Statement Compilation
Process Controls Placed in Operation
and Tests of Operating Effectiveness
for the Period October 1, 2004
through March 31, 2005
(D-2006-008)

Department of Defense
Office of Inspector General

Constitution of
the United States

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

Article I, Section 9

Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at <http://www.dodig.mil/audit/reports> or contact the Secondary Reports Distribution Unit, Audit Followup and Technical Support at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

DEPARTMENT OF DEFENSE

hotline

To report fraud, waste, mismanagement, and abuse of authority.

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.osd.mil www.dodig.mil/hotline



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

October 24, 2005

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

SUBJECT: Report on the Defense Departmental Reporting System and Related Financial Statement Compilation Process Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004 through March 31, 2005
(Report No. D-2006-008)

We are providing this report for 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 Mr. G. Marshall Grimes at (703) 428-1056 (DSN 328-1056). The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

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

Table of Contents

Foreword	i
Section I	
Independent Service Auditors' Report	1
Section II	
Description of the Defense Departmental Reporting System and Related Financial Statement Compilation Process Operations and Controls Provided by the Defense Finance and Accounting Service and the Defense Information Systems Agency	15
Section III	
Control Objectives, Control Activities, and Tests of Operating Effectiveness	27
Section IV	
Supplemental Information Provided by the Defense Information Systems Agency	171
Acronyms and Abbreviations	175
Report Distribution	177

FOREWORD

This report is intended for the use of DFAS and DISA management, its user organizations, and the independent auditors of its user organizations. Department of Defense personnel who manage and use the Defense Departmental Reporting System (DDRS) will also find this report of interest as it contains information about DDRS general and application controls.

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

The DDRS provides tools for DoD financial managers to produce audited financial statements, unaudited interim financial statements, and budgetary reports. The mission of DDRS is to standardize the departmental reporting process, produce financial statements and budgetary reports based on Federal requirements and standard attributes, and replace legacy departmental and command-level reporting processes.

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

Section I: Independent Service Auditors' Report



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

October 24, 2005

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

SUBJECT: Report on the Defense Departmental Reporting System and Related
Financial Statement Compilation Process Controls Placed in Operation and Tests of
Operating Effectiveness for the Period October 1, 2004 through March 31, 2005

We have examined the accompanying description of the Defense Departmental Reporting System (DDRS) general computer and application controls and the related financial statement compilation process (Section II). DDRS and the financial statement compilation process are sponsored and used by the Defense Finance and Accounting Service (DFAS). The DDRS system is jointly maintained and technically supported by DFAS and the Defense Information Systems Agency (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 DDRS user organization's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user organizations applied those aspects of internal control contemplated in the design of the controls at DFAS and DISA; and (3) such controls had been placed in operation as of March 31, 2005.

The control objectives were specified by the Department of Defense, Office of Inspector General (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.

The accompanying description includes only those general computer and application control objectives and control activities related to the unclassified aspects of DDRS and its related operations. Also, the accompanying description includes those general computer and application control objectives and control activities related to the receipt and processing of financial data from user locations, but does not include general computer and application controls related to the systems that generate and submit user financial data to DDRS. In addition, the accompanying description includes those general and application control objectives and related control activities applicable to the "DDRS Audited Financial Statements Module" (DDRS-AFS), the "DDRS Data

Collection Module” (DDRS-DCM), and the related financial statement compilation process, but does not include such objectives and activities related to the “DDRS Budgetary Module” (DDRS-B). The accompanying description includes only those general control objectives and related controls resident at DFAS centers in Arlington, Virginia; Cleveland, Ohio; Indianapolis, Indiana; and the DISA Defense Enterprise Computing Center (DECC) at Ogden, Utah. Further, the accompanying description includes only those application control objectives and related control activities resident at the DFAS centers located at Arlington, Virginia; Cleveland and Columbus, Ohio; Denver, Colorado; and Indianapolis, Indiana.

Our examination was conducted for the purpose of forming an opinion on the description of the DDRS-AFS general and application controls at DFAS and DISA (Section II and the control activities described in Section III). Information about business continuity plans and procedures at DISA, as provided by DISA and included in Section IV, is presented to provide additional information to user organizations and is not a part of the description of controls at DFAS and DISA. The information in Section IV has not been subjected to the procedures applied in the examination of the aforementioned description of the controls at DFAS and DISA related to DDRS-AFS and the related financial statement compilation process. Accordingly, we express no opinion on the description of the business continuity plans and procedures provided by DISA.

In performing our examination, we identified design deficiencies in five of 15 application control objectives (33 percent) that had been placed in operation as of March 31, 2005. The five identified design deficiencies were as follows:

Trial Balance Input to DFAS for Processing to DDRS-AFS

The accompanying description includes control activities related to DFAS processing of user organizations’ trial balances for input into DDRS-AFS. The description is based on the assumption that user organization trial balances received at DFAS may not be in full compliance with federal financial reporting requirements; thus requiring adjustment prior to upload to DDRS-AFS. DFAS controls were designed to derive certain proprietary accounts from budgetary accounts, usually from the “Report on Budget Execution and Budgetary Resources (SF-133),” and, at DFAS-Denver, some budgetary accounts were derived from proprietary accounts. As certain user organizations improve their accounting and reporting systems and processes, some or all of their submitted data may be accurately presented and may not require adjustment prior to upload to DDRS-AFS based on the prescribed derivation assumptions. Also, DFAS processing and revision of user accounting information for input to DDRS-AFS was not designed to provide appropriate segregation of duties at the DFAS centers in Cleveland, Ohio; Columbus, Ohio; and Denver, Colorado. There was no formal acceptance of user organization trial balances at these DFAS centers. Further, for these DFAS centers, the processes for preparing the trial balances for input were not approved by either the center or DFAS-Arlington.

As a result, the design of controls did not provide reasonable assurance that the control objective, “Controls provide reasonable assurance that trial balance data manually migrated into DDRS-AFS is accurate, authorized, and complete, and that data from the Report on Budget Execution and Budgetary Resources (SF-133), or other feeder systems, is input accurately into DDRS-AFS, and any reclassifications are authorized, approved, and monitored by an audit trail,” was achieved (Local Unique Processes control objective # 1).

Trading Partner Eliminations

The accompanying description includes control activities related to the elimination in DDRS-AFS of trading partner transactions as part of the process of consolidating the

Department's financial statements. However, the trading partner elimination process was based on the inability of certain user organizations in DoD to reconcile data from the buyer and seller in most intragovernmental transactions at the transaction level. Therefore, DFAS developed controls for the eliminations process in DDRS-AFS that relied on the seller-side of these transactions, adjusting the buyer-side data to agree with the seller-side data at a summary level. This process was established in DoD Financial Management Regulation (FMR), Volume 6B, Chapter 13. However, the DDRS-AFS process of relying on seller-side data was not designed to include controls for reconciling differences between seller-side data and buyer-side data at the transaction level.

As a result, the design of controls did not provide reasonable assurance that the control objective, "Controls are in place to ensure that trading partner data are supported by adequate documentation or valid estimating methodology. Controls provide reasonable assurance that DDRS has processes for determining the integrity of data flowing through the system, and trading partners are input and updated completely and accurately. Reports can identify the impact of trading partners on statement presentation," was achieved (Audited Financial Statements Module control objective # 4).

Trial Balance Input to DDRS-AFS and DFAS Center-Level User Access

The accompanying description includes control activities related to the input of trial balances and adjustments into DDRS-AFS. However, the description did not include controls to ensure that adjustment of beginning and ending balances were reviewed and approved. Users could circumvent the journal voucher approval process by posting adjustments to trial balances.

As a result, the design of controls did not provide reasonable assurance that the control objective, "Controls provide reasonable assurance that data transmissions between DDRS and user organizations are authorized, complete, accurate, and secure," was achieved (Audited Financial Statements Module control objective # 6).

The accompanying description includes control activities related to user access to DDRS-AFS. However, controls were designed to provide for access to DDRS-AFS on a center-level basis, instead of by responsible work area.

As a result, users may be provided access to more information than they actually need to conduct their assigned functions. DoD Instruction 8500.2, "Information Assurance (IA) Implementation," at Attachment 4 to Enclosure 4, "Enclave and Computing Environment, ECLP-1," "Least Privilege," states that access procedures enforce the principles of separation of duties and "least privilege."

As a result, the design of controls did not provide reasonable assurance that the control objective, "Unbalanced trial balances are flagged, but not reported until in balance. Controls provide reasonable assurance that application users are appropriately identified and authenticated, and that access to the application and output is restricted to authorized users for authorized purposes. Controls provide reasonable assurance that trial balances input is accurate and recorded in the proper period," was achieved (Audited Financial Statements Module control objective # 6).

United States Standard General Ledger Account Maintenance

The accompanying description includes control activities related to United States Standard General Ledger (USSGL) account maintenance control. However, DDRS-AFS controls did

not preclude USSGL reference and reporting table changes from being made in the production environment during periods of high activity. Changes or updates to the DDRS-AFS reference and reporting tables were made at the same time users were entering live data. Changes or updates to the USSGL reference and reporting tables during peak processing periods such as quarterly reporting cycles increased the risk that balances may be entered inaccurately. Additionally, the DDRS Program Management Office (PMO) did not have a documented review and approval process in place to verify the accuracy and completion of changes to the USSGL that were requested by DFAS-Arlington.

As a result, the design of controls did not provide reasonable assurance that the control objective, "Controls provide reasonable assurance that only valid and accurate changes are made to DDRS reference tables, Department reporting tables, and other critical system components; these changes are input and processed timely. Controls provide reasonable assurance new accounting line items are promptly added to the reference tables and obsolete accounts are promptly removed, and only valid accounts are added to the reference table," was achieved (Audited Financial Statements Module control objective # 7).

Data Collection Module

The accompanying description includes control activities related to determining the integrity of data flowing from the Data Collection Module (DCM) to DDRS-AFS. However, the design of controls allowed DDRS-AFS users in Columbus, Ohio and Indianapolis, Indiana to circumvent embedded controls by rekeying DCM data into DDRS-AFS instead of using the automated interface function. There was no requirement that these balances be marked "approved" prior to being rekeyed into DDRS-AFS. At DFAS-Indianapolis, balances were not approved before they were rekeyed into DDRS-AFS. This circumvention of controls increased the risk of erroneous data being entered into DDRS-AFS.

As a result, the design of controls did not provide reasonable assurance that the control objective, "Controls provide reasonable assurance that DDRS has systems or processes for determining the quality and integrity of data flowing through the system, and balances are input and updated completely and accurately," was achieved (Data Collection Module Interfacing control objective #1).

In our opinion, the accompanying description of general computer and application controls at DFAS and DISA related to DDRS-AFS and the related financial statement compilation process (Section II and the control activities in Section III) presents fairly, in all material respects, the relevant aspects of the controls at DFAS and DISA that had been placed in operation as of March 31, 2005. Also, in our opinion, except for the matters described in the preceding paragraphs, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of the controls at DFAS and DISA.

In addition to the procedures that we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specified controls, listed in Section III, to obtain evidence about their effectiveness in meeting the related control objectives described in Section III, during the period from October 1, 2004 to March 31, 2005. The specific control objectives; controls activities; and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to DDRS user organizations and to their auditors to be taken into consideration, along with information about the user organizations' internal control, when making assessments of control risk for user organizations.

In performing our examination, we identified deficiencies in operating effectiveness in eight of 15 application control objectives (53 percent), and in 32 of 82 general computer control objectives (39 percent) placed in operation for the period October 1, 2004 to March 31, 2005, as follows:

Journal Vouchers

As discussed in the accompanying description of controls, a purpose of DDRS-AFS is to produce auditable financial statements in accordance with the Chief Financial Officers (CFO) Act of 1990, the Government Management Reform Act (GMRA) of 1994, and the Federal Financial Management Integrity Act (FFMIA) of 1996. The use of journal vouchers aids immeasurably in producing the financial statements. Journal vouchers adjust for errors, record accounting entries that have not already been recorded, and are used for month-end closing and year-end processing and closing purposes. To a significant extent DDRS-AFS journal vouchers were either not supported at all or lacked sufficient supporting documentation. The DoD OIG previously reported unsupported accounting entries as a material weakness for the Department of Defense (DoD OIG Report No. D-2005-017, Independent Auditor's Report on the Fiscal Year 2004 DoD Agency-Wide Financial Statements, November 12, 2004).

DDRS-AFS had three categories of journal vouchers that were unsupported accounting entries; these were elimination balancing, adjustments to balance or reconcile in AFS (such as budgetary to proprietary accounts), and adjustments of trial balances to agree with budgetary status of funds reports. All three categories of unsupported journal vouchers had the effect of forcing agreement of amounts without actual, credible reconciliation of the two data sources at the transaction level (enabling subsequent corrective actions). These journal vouchers only provided the appearance of reconciliation between the data sources without actually achieving auditable reconciliation. User organizations' systems and processes did not provide sufficient information to DDRS-AFS to enable an efficient reconciliation, and the time pressures related to the financial statement preparation process did not provide adequate time for the extensive manual reconciliation processes required to prepare and process appropriate correcting adjustments to the transactions. Also, some journal vouchers were not approved by the appropriate level of authority (established by Chapter 2, Volume 6A, of the FMR) prior to entry into AFS. DFAS staff informed us that if they followed FMR policy on journal voucher approval authority, the financial statements would not be completed by the due dates. However, the entry of journal vouchers into DDRS-AFS without appropriate review and approval could result in the entry of unsupported journal vouchers.

As a result, the control objective, "Controls provide reasonable assurance that Journal Vouchers are supported by adequate documentation and that Journal Vouchers are approved prior to entry into a DDRS table; that there are segregation of duties in the preparation of Journal Vouchers; and that Journal Vouchers are in balance prior to entry into DDRS-AFS," may not have been achieved during the period from October 1, 2004 to March 31, 2005 (Audited Financial Statements Module control objective # 3).

Preparation of Financial Statements

As discussed in the accompanying description of controls, a purpose of DDRS-AFS is to produce auditable financial statements in accordance with the CFO Act of 1990, the GMRA of 1994, and the FFMIA of 1996. However, DoD policies related to the preparation of financial statements and the template used for preparation of financial statements did not

provide for reporting a significant amount of accounting information required by the Federal Accounting Standards Advisory Board (FASAB) and Office of Management and Budget (OMB) Bulletin 01-09. Also, the mapping of accounts for the preparation of financial statements in several instances relied on DoD general ledger accounts, instead of USSGL account codes. Further, the mapping of accounts used for the preparation of the Statement of Custodial Activity did not conform to Treasury requirements. In addition, there were multiple users with access to the beginning balance change role that allowed these users to override beginning balances that were carried forward in DDRS-AFS.

As a result, the control objective, “Controls provide reasonable assurance that financial statements and related footnotes are produced in conformance with the reporting requirements of FASAB, OMB Bulletin 01-09, and Treasury Financial Management Service. Controls provide reasonable assurance financial statements are complete, reporting all material financial information required by FASAB, and that automated totals in the financial statements are appropriately calculated,” may not have been achieved during the period October 1, 2004 to March 31, 2005 (Audited Financial Statements Module control objective # 1).

Audit Trails

As discussed in the accompanying description of controls, a purpose of DDRS-AFS is to produce auditable financial statements. A key element in the auditability of financial statements is the effectiveness of audit trails that allow external auditors to trace reported amounts to supporting documentation. In DDRS-AFS, although system audit logs were captured and available for review, such logs were not reviewed on a regular basis.

As a result, the control objective, “Controls provide reasonable assurance that DDRS-AFS produces financial statements that are supported by audit trails that are adequate for the financial management entity and external auditors to trace amounts reported in the financial statement back to trial balances and data from feeder systems. Controls provide reasonable assurance that audit trails indicate the user inputting the trial balance and the user approving the trial balance. All audit trails indicate the user inputting the Journal Voucher and the user approving the Journal Voucher. Audit trails are reviewed on a regular basis for appropriateness,” may not have been achieved during the period from October 1, 2004 through March 31, 2005 (Audited Financial Statements Module control objective # 2).

Validation Controls

As discussed in the accompanying description of controls, a purpose of DDRS-AFS is to produce auditable financial statements. The identification of erroneous data in trial balances and journal vouchers, and the correction of such data, are key elements in the auditability of financial statements. Although DDRS-AFS validation controls identified potentially erroneous data during reconciling processes, such data was not always communicated to the client.

As a result, the control objective, “Controls provide reasonable assurance that DDRS has processes for determining the integrity of data flowing through the system, and trial balances are input and updated completely and accurately. Controls provide reasonable assurance that data validation and editing are performed to identify erroneous data, and that erroneous data are captured, reported, investigated, and corrected,” may not have been achieved during the period from October 31, 2004 through March 31, 2005 (Audited Financial Statements Module control objective # 5).

DDRS and DISA DECC-Ogden System Security Authorization Agreements

As discussed in the accompanying description, DoD Instruction 5200.40, “Department of Defense Information Technology Security Certification and Accreditation Process” (DITSCAP) establishes a standard, department-wide process to certify and accredit information systems. The DDRS-AFS application and the DISA system enclave that supports the application each have a separate System Service Authorization Agreement (SSAA). However, the SSAA for DISA DECC-Ogden was not kept up to date in accordance with DITSCAP standards and the DDRS SSAA was not complete.

As a result, the following control objective, “The security plan is kept current,” may not have been achieved during the period from October 1, 2004 to March 31, 2005 (General Computer Controls control objective # 3).

System Authorization Access Request Forms

As discussed in the accompanying description, DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” requires access control mechanisms to ensure that data is accessed and changed only by authorized individuals and that registration to receive a user ID includes authorization by a supervisor. The “System Authorization Access Request (SAAR)” form¹ was designed to control user access to DDRS. However the SAAR form was not always completed or omitted critical information. For example:

- SAAR forms were not always authorized by the Information Assurance Officer.
- SAAR forms were not always authorized by the Functional Data Owner (FDO).
- One DDRS user did not have a SAAR form on file.
- For some users, the type of access granted to DDRS was inconsistent with the type of access authorized on the SAAR form.
- Prior to 2004, the SAAR form did not contain enough detail to indicate specific DDRS-AFS and DDRS-DCM roles. Previously submitted SAAR forms had not been revised or updated to conform to existing access requirements and some SAAR forms were missing required information, such as the justification for access or the type of access requested.

As a result, the following control objectives may not have been achieved during the period from October 1, 2004 to March 31, 2005:

- “Hiring, transfer, termination, and performance policies address security” (General Computer Controls control objective # 9);
- “Resource owners have identified authorized users and their access authorized” (General Computer Controls control objective # 19); “Adequate logical access controls have been implemented at the application and Operating System layer” (General Computer Controls control objective # 25);
- “Access is restricted to data files and software programs” (General Computer Controls control objective # 28);
- “Access settings have been implemented in accordance with the access authorizations established by the resource owners” (General Computer Controls control objective # 29);

¹ Reference to the SAAR form includes DD form 2875, DISA Form 41, and DISA and DFAS modified versions of the SAAR form.

- “Group authenticators for application or network access may be used only in conjunction with an individual authenticator” (General Computer Controls control objective # 44);
- “Access to program libraries is restricted to appropriate personnel” (General Computer Controls control objective # 65);
- “Policies and techniques have been implemented for using and monitoring the use of system utilities” (General Computer Controls control objective # 72);
- “Controls provide reasonable assurance that data transmissions between DDRS-AFS and user organizations are authorized, complete, accurate, and secure” (Audited Financial Statements control objective # 6);
- “Controls provide reasonable assurance that only valid and accurate changes are made to the DDRS-AFS Reference Tables, Department Reporting Tables and other critical system components; these changes are input and processed timely. Controls provide reasonable assurance that new accounting line items are promptly added to the reference tables and obsolete accounts are promptly removed, and only valid accounts are added to the reference tables” (Audited Financial Statements control objective # 7);
- “Controls provide reasonable assurance that balances entered into the DDRS-DCM are supported by adequate documentation, and that balances entered into the DDRS-DCM are approved prior to entry into a DDRS table” (Data Collection Module control objective # 2); and
- “Controls provide reasonable assurance that data transmissions between DDRS-AFS and DDRS-DCM are authorized, complete, accurate and secure. Unbalanced trial balances are flagged and not reported until in balance” (Data Collection Module Interfacing control objective # 2).

Database Administrator Segregation of Duties

As discussed in the accompanying description, DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” requires that change controls for software development be in place to prevent unauthorized programs or modifications to programs from being implemented and application programmer privileges to change production code and data be limited. The DDRS database administrators located at DFAS-Indianapolis had full access to the DDRS test, development, and production environments.

As a result, the following control objective, “Access to program libraries is restricted to appropriate personnel,” may not have been achieved during the period from October 1, 2004 to March 31, 2005 (General Computer Controls control objective # 65).

Training

As discussed in the accompanying description, DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” requires that DoD users and systems support personnel participate in periodic security awareness training. However:

- The system administrator training materials used at DISA DECC-Ogden were outdated.
- Some DDRS users in DFAS-Cleveland had not attended required security awareness training.

As a result, the following control objectives may not have been achieved during the period from October 1, 2004 to March 31, 2005:

- “Employees have adequate training and expertise” (General Computer Controls control objective # 10); and
- “A program is implemented to confirm that on arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned Information Assurance responsibilities” (General Computer Controls control objective # 11).

Audit Trail Access

As discussed in the accompanying description, DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” requires that access to system audit trails be restricted to only authorized users. DFAS-Indianapolis was unable to provide a system-generated listing of personnel that were assigned access to the privileged role with access to the DDRS application and database audit trails. Without this listing, the appropriateness of access to application and database audit trails could not be determined.

As a result, the control objective, “The contents of audit trails are protected against unauthorized access, modification or deletion,” may not have been achieved during the period from October 1, 2004 to March 31, 2005 (General Computer Controls control objective # 33).

Standard Operating Procedures

As discussed in the accompanying description, DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” requires that significant system administration functions and procedures be documented. Standard operating procedures to guide DISA DECC-Ogden system administrators in performing their job responsibilities were not documented.

As a result, the control objective, “Formal procedures guide system management personnel in performing their duties,” may not have been achieved during the period from October 1, 2004 to March 31, 2005 (General Computer Controls control objective # 80).

Physical Access Controls

As discussed in the accompanying description, DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” requires DoD Agencies to have physical access controls in place to restrict unauthorized access, and to have policies and procedures in place governing visitor access. DFAS-Cleveland was a tenant in a Federal building that was also occupied by other Federal entities. Although the main entrance to the building was monitored in accordance with government procedures, the floors occupied by DDRS software development and support staff were not restricted from access by other building tenants or authorized visitors. In addition, procedures governing visitor access to the building were not documented, some visit request letters were missing, and the DFAS-specific visitor sign-in sheet was not maintained.

As a result, the following control objectives may not have been achieved during the period from October 1, 2004 to March 31, 2005:

- “Adequate physical security controls have been implemented” (General Computer Controls control objective # 22); and
- “Visitors are controlled” (General Computer Controls control objective # 24).

Monitoring Audit Logs

As discussed in the accompanying description, DoD Instruction 8500.2, "Information Assurance (IA) Implementation," requires the regular review of audit trail records for indications of inappropriate or unusual activity. However, DISA DECC-Ogden did not proactively monitor or review operating system audit trails.

As a result, the following control objectives may not have been achieved during the period from October 1, 2004 to March 31, 2005:

- "Tools are available for the review of audit records and for report generation from audit records" (General Computer Controls control objective # 34); and
- "Policies and techniques have been implemented for using and monitoring the use of system utilities" (General Computer Controls control objective # 72).

Software Change Controls

As discussed in the accompanying description, DoD Instruction 8500.2, "Information Assurance (IA) Implementation," requires that authorizations for application or operating software changes be documented and maintained. However:

- Some software changes made by DFAS-Cleveland did not have required documentation and authorization signatures on file, including Statement of Agreement documents from the Functional Requirements Review (FRR), Test Readiness Review and Systems Integration Testing (TRR/SIT), Test Readiness Review and Functional Validation Testing (TRR/FVT), and Release Implementation Readiness Review.
- Software changes implemented by DFAS-Indianapolis on the production servers could not be traced back to authorized development activities conducted by DFAS-Cleveland.

As a result, the following control objectives may not have been achieved during the period from October 1, 2004 to March 31, 2005:

- "A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place" (General Computer Controls control objective # 14);
- "Authorizations for software modifications are documented and maintained" (General Computer Controls control objective # 59);
- "Changes are controlled as programs progress through testing to final approval" (General Computer Controls control objective # 61);
- "Emergency changes are promptly tested and approved before being moved into production" (General Computer Controls control objective # 62); and
- "Distribution and implementation of new or revised software is controlled" (General Computer Controls control objective # 63).

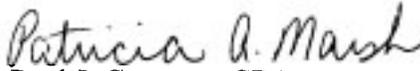
In our opinion, except for the matters described in the preceding paragraphs, the controls that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section III were achieved during the period from October 1, 2004 to March 31, 2005. However, the scope of our

engagement did not include tests to determine whether control objectives not listed in Section III were achieved; accordingly, we express no opinion on the achievement of control objectives not included in Section III.

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

The description of the controls at DFAS and DISA is as of March 31, 2005 and information about tests of their operating effectiveness covers the period from October 1, 2004 to March 31, 2005. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the system in existence. The potential effectiveness of specific controls at DFAS and DISA is subject to inherent limitations and, accordingly, errors or fraud may occur but 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 DDRS management, DDRS user organizations, and the independent auditors of such user organization.

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 Departmental Reporting System
and Related Financial Statement Compilation Process Operations
and Controls Provided by the Defense Finance and Accounting
Service and the Defense Information Systems Agency**

II. Description of Defense Departmental Reporting System and Related Financial Statement Compilation Process Operations and Controls Provided by the Defense Finance and Accounting Service and the Defense Information Systems Agency

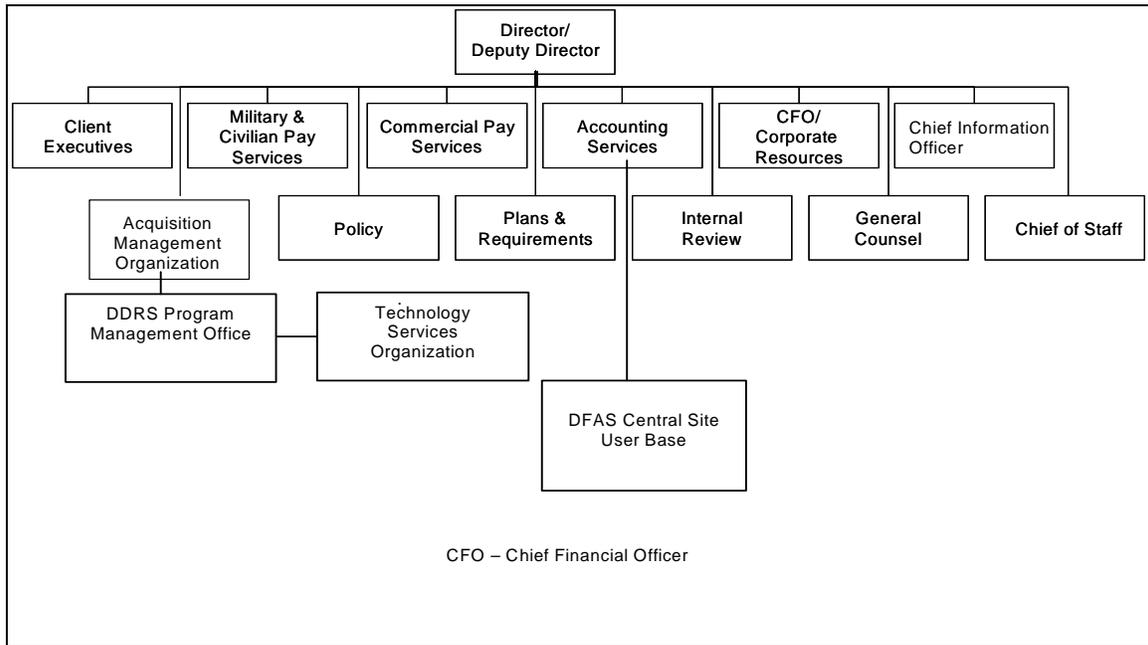
A. Overview of Operations

Department of Defense

The Department of Defense (DoD) is the cabinet-level agency responsible for establishing and administering defense initiatives and strategy for the United States. DoD employs approximately two million military and civilian individuals and has an annual operating budget of \$371 billion. The DoD is organized such that the Joint Chiefs of Staff, the Office of Inspector General, and each of the Military Departments report to the Office of the Secretary of Defense.

Defense Finance and Accounting Service

The DFAS mission is to provide responsive, professional finance and accounting services for the DoD. The Director of DFAS reports to the Under Secretary of Defense (Comptroller/Chief Financial Officer). DFAS is responsible for the proper accounting of resources in DoD. DFAS is organized such that the Director and Deputy Director oversee operations as depicted below:



In the Accounting Systems Directorate, Installation and Tactical Support Accounting Systems Organization, the Program Management Office (PMO) helps to ensure continued operation of the Defense Departmental Reporting System (DDRS) in accordance with DoD security and operational requirements. The Technology Services Organization (TSO) is responsible for elements of the technical administration of DDRS and provides multi-tier system support in coordination with other organizations. The TSO carries out its responsibilities for many aspects of system support in coordination with the Centralized Directorate for Information Management

(CDOIM), as well as decentralized Defense Office of Information Management (DOIM) organizations servicing other DFAS sites. CDOIM and DOIM groups are responsible for overall management and continuance of the DDRS computer processing operations. See the Information Systems and Control Environment discussions for detailed descriptions of PMO, TSO, CDOIM, and DOIM organizational roles relating to DDRS administration and operation.

Defense Information Systems Agency

DISA is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric (systems with operations distributed across a network) solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components under all conditions of peace and war.

DISA performs the following functions in support of the DDRS underlying information technology architecture:

- Installation and maintenance of system software, including operating systems, communication networks, and file control software;
- Installation and maintenance of the Oracle database management software;
- Administration of system parameter settings in the Oracle software that provide logical access control;
- Restriction of physical access to computer facilities, application programs, and data files housed in the facility;
- Backup and contingency planning, including maintenance of off-site processing capabilities and rotational off-site storage of critical files; and
- Logical segregation of major applications from other systems resident on the domain hardware and from unauthorized external users.

By providing the services and fulfilling the responsibilities outlined above, DFAS and DISA represent service organizations that act in concert to provide finance and accounting services supported by information systems and technology to DoD user organizations, including:

- Army Posts, Camps and Stations, such as Fort Riley and Fort Belvoir;
- Air Force, Security Assistance – DFAS-Denver;
- Defense Commissary Agency – Worldwide;
- Other Defense Agencies, such as the Defense Advanced Research Projects Agency; and
- DFAS field sites, including Pearl Harbor, Hawaii; San Antonio, Texas; Indianapolis, Indiana; Orlando, Florida; Rome, New York; Lawton, Oklahoma; and Seaside, California.

DISA's relationship with DFAS is, itself, a service organization and user organization relationship. DISA provides platform hosting and systems and hardware support services to DFAS, a user and administrator of the DDRS application resident on the DISA-operated platform. However, for the purposes of the Statement on Auditing Standards (SAS) 70/88 examination, DISA and DFAS are viewed as a combined service organization that delivers information systems technology-enabled finance and accounting support services.

B. Relevant Aspects of the Control Environment, Risk Assessments, and Monitoring

Control Environment

Defense Finance and Accounting Service. DFAS Acquisition Management Organization (DFAS-AMO) provides management control and coordination in DoD and has overall responsibility for the DDRS system, including reviewing and maintaining the DDRS security policy. The DDRS Program Management Office (PMO) provides program oversight, testing, training, data development, and customer service. The DFAS Technology Services Organization, Pensacola, Florida (DFAS-TSO-PE) provides a customer contact center that enters, logs, and tracks customer trouble tickets. The DFAS-TSO, located in Cleveland, Ohio (DFAS-TSO-CL) provides DDRS software engineering and technical support. The Technology Services Organization Corporate Services in Indianapolis, Indiana (DFAS-TSO-CS), provides production support and database administration.

Accounting office employees and contractors are required to review applicable administrative orders, policies, and procedures with the Human Resource Office and must complete appropriate forms to gain access to DFAS systems. The Information Security Manager: (1) provides basic systems security awareness training, (2) secures civilian and contractor signatures on the ADP Security Awareness disclosure, (3) identifies the Terminal Area Security Officer to the employee and explains the Terminal Area Security Officer's responsibilities; and (4) notifies appropriate personnel to provide employee or contractor access or to immediately terminate access to DFAS Automated Information System (AIS) resources when an employee or contractor processes in or out. The accounting and DFAS-TSO-CL facilities do not require employees to have security clearances before beginning employment.

DFAS employees have formal job descriptions. Contractors' duties and deliverable descriptions, as well as required skills and security levels, are identified in commercial contracts.

DDRS Development and Management activities follow Software Quality Assurance (SQA) functions and controls adhering to the DoD and DFAS standards established for that purpose. When implementing the DDRS SQA function, management considered two sets of controls. First, at the management level, they monitor the definition and establishment of six SQA reviews occurring at specific points in the life cycle of a given DDRS Release. These reviews constitute milestones providing the opportunity to assess the executed work for a specific phase in the development process. The reviews ensure the identification of major discrepancies and risks, necessary conditions to complete the current phase are satisfied, and conditions necessary to proceed to the next phase are in place. Second, at the development level, controls consist of a set of DDRS policies that have been developed to define engineering practices, determine development behavior, specify procedures consistent with standard engineering practices in adherence to the Software Engineering Institute's Capability Maturity Model framework, and meet SQA objectives and management requirements.

DFAS has formal capital planning and programming processes. Annually, the DFAS Portfolio Management Directorate requires the DDRS Program Management Office (PMO) to submit a Portfolio Management Initiative Report. The Management Directorate conducts a review to ensure the project continues to support DFAS' strategic objectives. In addition, the Office of the Secretary of Defense, Program Analysis and Evaluation, reviews and approves a five-year program objective memorandum describing the program's Planning, Programming, Budgeting, and Execution.

Defense Information Systems Agency. A signed Service Level Agreement (SLA) between DISA and DFAS documents the support services provided by DISA to DDRS. Both agencies review and update the SLA annually. The Defense Enterprise Computing Center (DECC) located at Ogden, Utah maintains and executes the DDRS system on mid-tier platforms. DISA DECC-Ogden is part of the Center for Computing Services in the Global Information Grid Combat Support Directorate, a DISA Strategic Business Unit.

The DISA Security Manager completes the processing and vetting of all new employees and contractors accessing the DISA facility in Ogden. DISA employees have formal job descriptions. Contractors' duties and deliverable descriptions are identified in commercial contracts. Contracts also specify the skills and security levels required for contract staff. All contractors and employees are required, at a minimum, to have a Secret clearance and a positive National Agency Check.

All new employees must sign DISA Form 312, which serves as a nondisclosure agreement for sensitive and classified information. Terminated employees are also required to re-sign the Form 312 to acknowledge that they understand the agency policies for sensitive and classified information. The contracting officer is responsible for confirming that all contractors assigned to DISA DECC-Ogden have a valid contract to operate at that location and the Security Manager confirms the length of the contract and determines when system accounts should expire. All new employees and contractors are required to complete DD Form 2875, "System Authorization Access Request (SAAR)," to gain access to DISA systems and must complete security awareness training.

Risk Assessments

DoD Instruction 5200.40, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," establishes a standard Department-wide process, set of activities, general tasks, and management structure to certify and accredit information systems. This process maintains the information assurance and security posture of the defense information infrastructure throughout the life cycle of each system. The certification process is a comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards to establish the extent to which a particular design and implementation meets specified security requirements and covers physical, personnel, administrative, information, information systems, and communications security. The accreditation process is a formal declaration by the designated approval 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.

The DITSCAP process includes several activities that document and assess risks associated with DDRS. The DDRS application and the DISA system enclave that supports the application each have separate System Security Authorization Agreements (SSAA) as part of the DDRS DITSCAP process. Each SSAA is a living document that represents an agreement between the designated approval authority, certifying authority, user representative, and program manager. The DDRS SSAA documents its mission description and system identification, environment description, system architecture description, system class, system security requirements, organizations and resources, and the DITSCAP plan. On a periodic basis, the system security officer verifies and validates DDRS compliance with information in the SSAA. These verification and validation procedures include, among other steps, vulnerability evaluations, security testing and evaluation, penetration testing, and risk management reviews. DDRS was certified and accredited by DFAS on December 3, 2002.

The DDRS application and enclave SSAAs document threats to DDRS and its supporting technical environment. The SSAAs also contain Residual Risk Assessments that document vulnerabilities noted during DDRS tests and analyses. Management updates the SSAA periodically. Personnel from the Defense Finance and Accounting Service - Arlington (DFAS-Arlington), DFAS-TSO-CS, DFAS-TSO-CL, and the Defense Information Systems Agency (DISA) Defense Enterprise Computing Center (DECC) Ogden, Utah (DISA DECC-Ogden) participate in these risk assessments.

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 management, financial, and operational reports available to help monitor the performance of accounting processing as well as the DDRS system itself. Management periodically reviews these reports and takes action as necessary. The system logs and reports any procedural problems or exceptions to normal scheduled processing and management ensures that all issues are resolved in a timely manner. In addition, several other organizations in DoD perform monitoring associated with DDRS-related internal controls. These organizations include:

DFAS Internal Review Office

DFAS has an Internal Review Office that conducts internal audits, inspections, and investigations of the DFAS related system components that support DDRS. The DFAS Internal Review Office is independent of the DDRS management structure and does not manage, maintain, or configure DDRS systems.

DISA Office of the Inspector General and Field Security Office

DISA has an independent Office of the Inspector General that conducts internal audits, inspections, and investigations of DISA components that support DDRS. The Field Security Operations (FSO) unit periodically reviews DISA's security practices. DDRS system components maintained by DISA are subject to FSO reviews. The FSO is independent of the DECC-Ogden management structure and does not maintain or configure DDRS systems.

Department of Defense Office of Inspector General

Congress established the Department of Defense Office of Inspector General (DoD OIG) to conduct and supervise audits and investigations of DoD operations. The DoD OIG reports directly to the Secretary of Defense and is independent of DFAS and DISA. DDRS and the accounting processes it supports are part of the DoD OIG audit universe and are subject to financial, operational, and information technology audits.

C. Information and Communication

Information Systems

The DDRS provides tools for DoD accountants to produce audited financial statements, unaudited interim financial statements, and budgetary reports. The DDRS-AFS module produces the Statement of Budgetary Resources, Balance Sheet, Statement of Net Position, Statement of Net Cost, Statement of Financing, and the Statement of Custodial Activities. It also produces the interim and annual financial statement report footnotes, Management Reports, Required Supplementary Information (RSI), and Reconciliation Reports. The DDRS Budgetary module produces the Report on Budget Execution and Budgetary Resources (SF-133), Report on

Reimbursements (Supplemental 725), Appropriation Status By Fiscal Year, Program And Sub-accounts (DoD 1002), Accounting Report 1307 (AR 1307), Schedule of Transfers and Re-appropriations, and the Report on Receivables. DDRS-AFS and DDRS Budgetary report for both the Defense Working Capital and General Funds. The DDRS-DCM is a sub-module of DDRS-AFS. DDRS-DCM captures financial data from non-financial feeder systems to support the audited financial statements. DDRS-DCM collects data from the following functional reporting areas:

- Capital Leases
- Capitalized Assets
- Contingencies
- Deferred Maintenance Employee Benefits
- Environmental Liabilities – Non-Federal
- Federal Employees' Compensation Act (FECA)
- Imputed Costs
- Judgment Funds
- Operating Leases
- Operating Materials & Supplies (OM&S)
- Other Liabilities
- Personal Property
- Real Property, and
- Supplementary Stewardship Information

Defense Management Review Decisions 910 and 912 led to major cost-savings initiatives aimed at standardizing processes and consolidating finance and accounting operations and automated information systems (AISs). In November 1990, Congress passed the Chief Financial Officers (CFO) Act (Public Law 101-576, as amended) requiring DoD to improve financial management and reporting. Under Secretary of Defense Memorandum of October 13, 1993, “Accelerated Implementation of Migration Systems, Data, Standards, and Process Improvement,” directs Defense Agencies to select migration systems to be used for consolidating systems, and to achieve full implementation of migration systems across the same functions.

The Government Management Reform Act (GMRA) of 1994 requires federal agencies to submit audited financial statements to the Office of Management and Budget and the U.S. Treasury annually. The Federal Financial Management Improvement Act (FFMIA) of 1996 requires all Federal agencies to implement and maintain financial management systems that comply substantially with Federal financial management systems requirements, applicable Federal accounting standards, and the United States Standard General Ledger at the transaction level.

DDRS Support Functions

DFAS-Arlington provides management control and coordination in DoD and has overall responsibility for interpretation and application of DDRS. DISA DECC-Ogden maintains and executes DDRS on mid-tier platforms. The Technology Services Organization in Cleveland, Ohio, (DFAS-TSO-CL) which is part of DFAS, provides DDRS application technical support. The Technology Services Organization Corporate Services in Indianapolis, Indiana, (DFAS-TSO-CS) also a part of DFAS, provides DDRS database management and administrative support.

DDRS Functionality

The DDRS-AFS module produces the quarterly and annual CFO financial statements and the Federal Agencies Centralized Trial Balance System (FACTS I and II) reports for DoD. The DDRS-DCM captures financial data from non-financial feeder systems to support the CFO

financial statements. All DoD reporting entities are currently using the DDRS-DCM module. The DoD will standardize the budgetary reporting process and replace the legacy departmental budgetary reporting systems through the implementation of the DDRS Budgetary Module.

The component-level accounting information goes through several manual processes of adjustment at DFAS Centers before input to the DDRS-AFS Module. The DFAS centers put this accounting data through Microsoft Excel crosswalks to adjust it to common account codes compliant with the USSGL. The data is also analyzed to identify data quality problems, such as abnormal account balances, out-of-balance trial balances, and proprietary accounts not in balance with budgetary accounts. Several analytical processes are used to adjust accounting data for these problems. These manual processes may not be well established in policy and may vary from center to center. At the conclusion of these processes, the data is manually input to import sheets for transfer to DDRS-AFS. In the Centers where the Budgetary Module has been implemented, these processes are automated. The Budgetary Module has been implemented in the Kansas City Center (Marine Corps Working Capital Fund), the Cleveland Center (Navy Working Capital Fund), and the Denver Center (Air Force General Fund).

In addition to financial reporting, DDRS-AFS and DDRS-Budgetary provide the following functionality:

- report certification;
- journal voucher creation and approvals;
- memorandum creation and approvals;
- footnote creation and administration;
- financial statements and reports at lower levels;
- drill down on reports and footnotes;
- report export to Microsoft Word, Microsoft Excel, and Portable Document Format (PDF);
- reconciliation within and between reports;
- file transfer protocol or upload;
- data locking and certifying;
- data export;
- report map and crosswalk table maintenance;
- trend analysis and management reports;
- ad-hoc reporting capability;
- application security administration; and
- internal audit reporting.

DDRS has over 1,100 end users at over 100 locations. The user base consists of Accountants, Auditors, Budget Analysts, and Financial Analysts throughout the DoD Military Departments and Defense Agencies.

DDRS supports the financial reporting requirements of the DoD Comptroller and subordinate organizations. DDRS receives trial balance data from a variety of DoD accounting systems. The DDRS PMO distributes a DDRS chart of accounts with all USSGL transactions and attributes quarterly. DFAS accountants populate the charts of accounts and upload them to DDRS-AFS.

For those DFAS sites that have implemented the DDRS-Budgetary module, accountants upload data files from local accounting systems to DDRS-Budgetary. DDRS-Budgetary translates the data to the USSGL and related attributes. DDRS-Budgetary consolidates this data and produces program level trial balances that it delivers to DDRS-AFS. The Navy and Marine Corps Working Capital Funds and the Air Force General Fund have implemented DDRS. DFAS plans to implement DDRS-Budgetary for all budgetary reporting.

System Architecture

DDRS is a web-based architecture comprised of an application server on the front-end and a database server on the back-end, connected directly in the DISA DECC-Ogden enclave. These servers are connected to users and interfacing systems using the DoD-maintained networks comprised of Internet Protocol based services, such as the Non-Classified Internet Protocol Router Network. The network connects DDRS to a wide variety of DFAS and non-DFAS user sites (mainframes, mid-tiers, and personal computers) that supply or exchange data with DDRS primarily through electronic file transfers. Examples of external interface sites include the Standard Accounting, Budgeting and Reporting System (SABRES); and the U.S. Department of Treasury Federal Agencies Centralized Trial Balance System (FACTS) I and FACTS II.

DDRS programming languages include PLSQL, HTML, Oracle Designer, Oracle Developer, Oracle Reports and Java. The Oracle Application Server provides security protection mechanisms at entry points. DISA DECC-Ogden provides the web server that services all applications that support DDRS. This server accepts the users' secure web requests by supplying a menu screen with options for each application to the DDRS Logon Screen, where individuals enter their DDRS login user IDs and passwords.

Communication

The Service Level Agreement (SLA) documents the support relationship between DFAS and DISA DECC-Ogden. Management reviews and updates this document annually. The SLA outlines contacts and liaisons for use when DDRS issues arise. DISA DECC-Ogden also assigns a customer relationship manager to work with DFAS-TSO-CL to resolve any DDRS processing problems or concerns.

DFAS-TSO-CL and accounting office directors and managers meet weekly to discuss DDRS processing issues. There is also a Configuration Control Board, comprised of DFAS-TSO-CL, the DDRS PMO, and Accounting Office personnel, to review and approve functional and systemic changes to DDRS. The DDRS PMO maintains a help desk function to identify, track, and communicate DDRS user issues and problems to the DFAS-TSO-CL for resolution.

D. Control Objectives and Related Control Activities

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

User Organization Control Considerations.

The control activities at DFAS and DISA related to DDRS-AFS and the financial statement compilation process were designed with the assumption that certain controls would be placed in operation at user organizations. This section describes some of the controls that should be in operation at user organizations to complement the controls at DFAS and DISA.

User organizations are defined as those organizations that use DDRS for the preparation of their quarterly and annual financial statements. User organizations provide DDRS with general ledger trial balances and other financial data required for the preparation of financial statements. Generally, the application of specific control activities at user organizations is necessary to achieve certain control objectives included in Section III of this report. User auditors are to

consider whether these user organization controls have been placed in operation at the user organizations. The list of user organization controls presented below does not represent a comprehensive set of all the controls that should be employed. Other controls may be required at user organizations depending on the specific financial and accounting circumstances of the organization.

Controls to Mitigate the Effects of DoD Material Weaknesses

DDRS relies on user organizations to provide financial data, in the form of trial balances, as the basic information used in the preparation of financial statements. User organizations must have controls in place to provide reasonable assurance that financial information meets Federal requirements for preparation of financial statements. To the extent that user organization controls fail to achieve compliant trial balance information, the DDRS-produced financial statements will also be noncompliant.

Other User Organization Controls

The control activities at DFAS and DISA related to DDRS were designed with the assumption that certain controls would be in place 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 but is not a comprehensive list of all controls that user organizations should employ.

1. The financial closing and reporting process is documented in official policies and procedures and distributed to all employees. Any changes made to the established procedures must be authorized by management and communicated throughout the organization.
2. Roles and responsibilities in the financial closing and reporting process are clearly defined, documented, and communicated to all personnel.
3. General policies are established and documented regarding permissible overrides of existing policies and procedures for the financial closing and reporting process.
4. As part of the financial reporting process, management and responsible personnel identify all generally accepted accounting principles and federal reporting requirements affecting the entity.
5. Reconciliations for all significant accounts are performed and prepared timely and independently reviewed.
6. All required analyses are completed timely and reviewed for appropriate assumptions, methodology, and evaluation of results. Unusual items and exceptions are investigated, resolved and recorded in the correct accounting period.
7. All trading partner events and transactions are recorded, authorized, and disclosed in the correct accounting period.
8. All events and transactions requiring financial statement disclosure are identified, analyzed and prepared in accordance with generally accepted accounting principles and federal reporting requirements.
9. Disclosure checklists and instructions are used in preparing and reviewing all draft financial statements and disclosures for completeness and consistency.

10. All required financial statement disclosure reporting packages and analyses are prepared and independently reviewed prior to submission to DFAS for further processing in DDRS-AFS.

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

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

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

The information contained in this section was provided by several different entities:

- The control objectives were specified by the DoD OIG, and accepted by DFAS and DISA.
- The control activities were provided by DFAS and DISA.
- Section III was provided by DoD OIG.

The controls described and tested in this section are limited to those general and application control objectives and related control activities applicable to DDRS-AFS, DDRS-DCM, and the related financial statement compilation process. The controls related to DDRS-Budgetary were specifically excluded from this review. In addition, the controls related to the feeder systems that are the source of much of the information in DDRS-AFS are specifically excluded from this review. We did not perform procedures to evaluate the effectiveness of the input, processing, and output controls in DDRS-Budgetary or in these feeder systems, although we did perform procedures to evaluate DDRS-AFS interface input and output controls. We did not perform any procedures to evaluate the integrity and accuracy of the data contained in DDRS-AFS.

General Computer Controls

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
	<i>Enterprise-Wide Security Program Planning</i>			
1	Risks are periodically assessed.	<p><u>DISA DECC-Ogden</u> Automated Security Readiness Review (SRR) scripts are run on each server and reported to the Montgomery SRR database on a weekly basis. Each system has a SRR and an Internet Security Systems scan before it is connected to the network. The DISA Field Security Office, periodic SRRs, and Internet Security System Scans. DISA DECC-Ogden conducts reviews of the System Security Authorization Agreement (SSAA), which includes the operation facility environmental risk assessment that is renewed and reviewed on an annual basis.</p> <p><u>DFAS-Arlington</u> The DDRS application security risks are randomly sampled and analyzed every three years. These risks are reported to DFAS Information Assurance Management and are considered for accreditation and re-accreditation every three years.</p>	<p><u>DISA DECC-Ogden</u> Read the latest risk assessment included in the SSAA dated February 18, 2004, to confirm that risks were periodically assessed.</p> <p>Observed the SRR process to confirm that it occurred and that corrective actions were tracked.</p> <p>Inspected a single SRR performed by DISA DECC-Ogden and inspected the Vulnerability Management System findings report to confirm findings identified by the SRR had been addressed.</p> <p><u>DFAS-Arlington</u> Read the latest risk assessment included in the SSAA to confirm that risks were periodically assessed.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>
2	A security plan is documented and approved.	<p><u>DISA DECC-Ogden</u> DISA DECC-Ogden documents the security plan in the SSAA, which is renewed and approved on an annual basis.</p>	<p><u>DISA DECC-Ogden</u> Read the DISA DECC-Ogden SSAA to confirm that it included a current and approved security plan. Confirmed, through</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Arlington</u> A SSAA was created specifically for DDRS to obtain an approval to operate. The SSAA was approved on December 3, 2002.</p>	<p>inquiry of the Information Assurance Manager, the process for updating the DISA DECC-Ogden SSAA and that the SSAA had been updated.</p> <p><u>DFAS-Arlington</u> Read the DDRS SSAA to confirm it had been documented, updated, and approved.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>
3	The security plan is kept current.	<p><u>DISA DECC-Ogden</u> DISA DECC-Ogden documents the security plan in the SSAA. The security plan is renewed, reviewed, and approved on an annual basis.</p> <p><u>DFAS-Arlington</u> The DDRS SSAA is updated as needed and completely updated every three years for reaccreditation. The DDRS SSAA is in the process of being updated.</p>	<p><u>DISA DECC-Ogden</u> Read the DISA DECC-Ogden SSAA to confirm the security plan in the SSAA had been documented, updated, and appropriately approved.</p> <p>Read the following documents to confirm that each had been updated:</p> <ul style="list-style-type: none"> • DISA DECC-Ogden Systems Security Policy, • Security Requirements, and, • Certification Test and Evaluation Plan. <p><u>DFAS-Arlington</u> Read the DDRS SSAA to confirm it had been documented, updated and appropriately approved.</p>	<p><u>DISA DECC-Ogden</u> The DISA DECC-Ogden SSAA was not compliant with DITSCAP requirements. Specifically, the DISA DECC-Ogden SSAA had six incomplete appendices.</p> <p><u>DFAS-Arlington</u> The DDRS SSAA was not compliant with DITSCAP requirements. Specifically, the DDRS SSAA had 20 incomplete sections, seven missing sections, and one incomplete appendix.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>Confirmed through inquiry of the Information Assurance Manager on the process for updating the DDRS SSAA and that the DDRS SSAA had been updated.</p> <p>Read the following documents to confirm that each had been updated:</p> <ul style="list-style-type: none"> • DDRS Systems Security Policy, • Security Requirements, and • Certification Test and Evaluation Plan. 	
4	A security management structure has been established.	<p><u>DISA DECC-Ogden</u> An Information Assurance Manager and Alternate Information Assurance Manager have been assigned. There are Information Assurance Officers for each type of Operating System and Terminal Area Security Officers are assigned to each area.</p> <p><u>DFAS-Arlington</u> DDRS has an Information Assurance Officer, Assistant Information Assurance Officers, and an Information Assurance Manager.</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry that a management structure had been established.</p> <p>Read the DISA DECC-Ogden organizational chart and job descriptions to confirm that all positions were established in writing.</p> <p>Read the DISA DECC-Ogden SSAA to confirm that each security management position was outlined in the SSAA.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry that a management structure had been established.</p>	<p><u>DISA DECC-Ogden</u> The security management structure contained position titles that were not in accordance with DoD Instruction 8500.2 requirements.</p> <p>However, we confirmed through interviews and inspection of the organizational chart and job descriptions that a security management structure was in place. As such, the intent of the objective was achieved.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>Read the DDRS Program Management Office (PMO) organizational chart and job descriptions to confirm that all positions were established in writing.</p> <p>Inspected the Appointment Letters for the Information Assurance Officer, Assistant Information Assurance Officer, and the Information Assurance Manager to confirm that each had been appointed in writing with the responsibilities of their positions included in appointment letters.</p>	
5	Information security responsibilities are clearly assigned.	<p><u>DISA DECC-Ogden</u> The information security responsibilities are included in the security plan. Also the security handbook identifies roles and responsibilities.</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry that a management structure had been established.</p> <p>Read the DISA DECC-Ogden organizational chart and job descriptions to confirm that all positions were established in writing.</p> <p>Read the DISA DECC-Ogden SSAA to confirm that each security management position was outlined in the SSAA.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Arlington</u> The DDRS Information Assurance Officer, Assistant Information Assurance Officers, and Information Assurance Manager are appointed in writing with the responsibilities attached to the appointment letters.</p>	<p><u>DFAS-Arlington</u> Confirmed through inquiry that a management structure had been established.</p> <p>Read the DDRS PMO organizational chart and job descriptions to confirm that all positions were established in writing.</p> <p>Inspected the appointment letters for the Information Assurance Officer, Assistant Information Assurance Officer, and Information Assurance Manager to confirm that each had been appointed in writing with the responsibilities of their positions included in appointment letters.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>
6	<p>A set of rules that describe the Information Assurance operations of the DoD information system and clearly delineate Information Assurance responsibilities and expected behavior of all personnel is in place.</p>	<p><u>DISA DECC-Ogden</u> This is covered through the periodic compliance review of the UNIX Security Technical Implementation Guide (STIG), Network Infrastructure Security Technical Implementation Guide. https://iase.disa.mil/techguid/stig/index.html</p> <p>DISA also ensures each new DISA employee has received General and System Specific Rules of Behavior brief(s) from their immediate supervisor, has signed the acceptance form, and is cognizant of their responsibilities in safeguarding system</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry that a management structure had been established.</p> <p>Read the DISA DECC-Ogden organizational chart and job descriptions to confirm that all positions were established in writing.</p> <p>Read the DISA DECC-Ogden SSAA to confirm that each security management position was outlined in the SSAA.</p>	<p><u>DISA DECC-Ogden</u> Rules of Behavior forms were not available for the DDRS System Administrators.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>security prior to being given system access.</p> <p><u>DFAS-Arlington</u> The DDRS Appendix M - Personnel Controls and Technical Security Controls, which is part of the DDRS SSAA, provides detailed descriptions of the DDRS user roles. The Personnel Controls and Technical Security document also describes the roles and responsibilities of the DDRS Program Manager, Information Assurance Officer, Terminal Area Security Officer, Database Administrators, and DDRS user. Additionally, each DDRS user is also required to read and sign the DDRS Rules of Behavior that describes the rules each DDRS user is to follow.</p>	<p>Inquired with the Information Assurance Manager on the availability of the Rules of Behavior for the DDRS System Administrators.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry that a management structure had been established.</p> <p>Read the DDRS PMO organizational chart and job descriptions to confirm that all positions were established in writing.</p> <p>Read the Appointment Letters for the Information Assurance Officer, Assistant Information Assurance Officer, and the Information Assurance Manager to confirm that each had been appointed in writing with the responsibilities of their positions included in appointment letters.</p> <p>Read the DDRS SSAA to confirm that the security management position was outlined in the SSAA.</p> <p>Inspected all 18 Rules of Behavior forms to confirm that the forms were on file for the DDRS PMO staff.</p>	<p><u>DFAS-Arlington</u> Eight of 18 PMO users did not have Rules of Behavior forms on file.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
7	Owners and users are aware of security policies.	<p><u>DISA DECC-Ogden</u> DISA DECC-Ogden maintains the security awareness training program. This program requires each individual with network access to complete security awareness training on an annual basis.</p> <p><u>DFAS-Arlington</u> DDRS has a DDRS Rules of Behavior document. DDRS users must sign that they have reviewed and agreed to the rules in order to gain access to DDRS. Additionally, security awareness training for DFAS-Arlington is handled through a community page via ePortal. A database is in development to allow for better tracking of security awareness training completion.</p>	<p><u>DISA DECC-Ogden</u> Read the Security Awareness Training briefing slides provided by DISA DECC-Ogden.</p> <p>Inspected all six training sign-in sheets to confirm that DISA DECC-Ogden employees had attended annual security awareness training.</p> <p><u>DFAS-Arlington</u> Inspected all 18 Rules of Behavior forms to confirm that forms were on file for the DDRS PMO staff.</p> <p>Confirmed, through inquiry of the Information Assurance Manager, the process DFAS-Arlington maintained for security awareness training.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> Although security awareness training was performed, there was no documented process in place for tracking that security awareness training occurred and that DFAS personnel completed the training.</p>
8	An incident response capability has been implemented.	<p><u>DISA DECC-Ogden</u> The DISA Regional Computer Emergency Response Team located at Scott Air Force Base, IL is responsible for monitoring the intrusion detection system. This system governs DISA DECC-Ogden. Additional controls are in place to confirm that authorized and unauthorized network access is monitored through TCP Wrapper and Klaxon or Banshee. Host based Intrusion Detection System, Symantec Enterprise Security Manager, and Intruder Alert is installed on all UNIX servers. If an incident occurs, an</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inspection that the incident plan included in the DISA DECC-Ogden SSAA had been implemented. No random sample of items was selected for testing because there were no incidents involving DDRS during our testing period.</p> <p>Confirmed through inquiry of the Information Assurance Manager that a process was in place for reporting computer security incidents.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>e-mail is sent to the Information Assurance Officer and a report of the incident is drafted and sent to the appropriate personnel. Remedial action is then taken.</p> <p><u>DFAS-Arlington</u> DFAS has an incident response team that incidents are reported to. DDRS has an incident response plan that is posted on the DDRS web site. The DDRS Rules of Behavior informs users of the incident response plan. The incident response plan is posted on the DDRS web site at DFAS-CERT@DFAS.MIL.</p>	<p><u>DFAS-Arlington</u> Confirmed through inspection that the incident plan included in the DDRS SSAA had been implemented. No random sample of items was selected for testing because there were no incidents involving DDRS during our testing period.</p> <p>Inspected all 18 Rules of Behavior forms to confirm that forms were on file for the DDRS PMO staff.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>
9	Hiring, transfer, termination, and performance policies address security.	<p><u>DISA DECC-Ogden</u> To ensure DISA DECC-Ogden is operated and continues to be maintained in a secure, controlled manner such that its data and other connected systems are appropriately protected; the following personnel controls have been implemented:</p> <ul style="list-style-type: none"> -National Agency Check personal security investigations are performed for all functional users (civilian, military, and contractors), as a minimum. -Specified system and application permissions are granted that only allow access to required, need-to-know information. 	<p><u>DISA DECC-Ogden</u> Read the hiring, transfer, termination, and performance policies of DISA DECC-Ogden to confirm they were documented.</p> <p>Inspected all nine SAAR forms to confirm that a form was on file for all System Administrators with access to the DDRS Operating System.</p> <p>Confirmed through inquiry that a DISA DECC-Ogden employee was debriefed upon termination</p>	<p><u>DISA DECC-Ogden</u> Seven of nine SAAR forms inspected did not have the signatures of the Information Assurance Officer on the SAAR form.</p> <p>One System Administrator did not have a SAAR form on file. Additionally, access had not been removed for that user in a timely manner. This user's access was subsequently deleted because he no longer required access to DDRS.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>-Specific DECC system training is performed.</p> <p>-System Authorization Access Request (SAAR) forms are completed for all DECC system users.</p> <p>-Registration of all users by DECC System Administrators, Information Assurance Officer, or the specific data owners is performed.</p> <p>-Unique User ID and passwords are required for all users.</p> <p>-Initial and refresher Information Security training is conducted.</p> <p>Individuals requiring access to sensitive information are processed for access authorization.</p> <p>Only individuals who have a valid need-to-know are granted access.</p> <p>Comprehensive account management process is implemented to ensure only authorized users can gain access.</p> <p><u>DFAS-Arlington</u> DFAS has agency-wide policies and procedures in place for the hiring, transfer, and termination; and policies that address security clearance requirements. Additionally, the DDRS SSAA documents personnel screening requirements. Only personnel who have undergone the prescribed background investigation, commensurate with the designated position sensitivity, are granted access to DFAS information. The DFAS Human Resources Office</p>	<p>of employment and that a DISA Form 70 was used to document the collection of DISA DECC-Ogden property.</p> <p>Confirmed through observation that an e-mail had been sent to the System Administrator to request that system access be removed for a terminated employee.</p> <p>Inspected annual security awareness training sign-in sheets for nine DISA DECC-Ogden employees to confirm that each had completed security awareness training.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry that agency-wide policies and procedures were available for the hiring, transfer, and termination of DFAS personnel.</p> <p>Inspected all 18 SAAR forms to confirm that each form contained the justification for access, security clearance level, and was properly approved.</p>	<p><u>DFAS-Arlington</u> Three of 18 SAAR forms did not document justification for access completed; another three of 18 did not document type of system access.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>oversees the activities required for processing security clearance when necessary system-level privileges will be issued to DDRS users based on assigned roles and responsibilities.</p> <p>Only individuals who have a valid need-to-know are granted access. A comprehensive account management process has been implemented to ensure only authorized users can gain access.</p>		
10	Employees have adequate training and expertise.	<p><u>DISA DECC-Ogden</u> Training is conducted on a recurring basis using a variety of methods such as e-mail, Commanders Call, one-on-one training sessions, as well as block briefings. Personnel are scheduled for specific training on the Operating Systems and Administrative software for the systems within DISA DECC-Ogden on an as needed basis. All security-type training is reported monthly to the Field Security Office.</p> <p><u>DFAS-Cleveland</u> Every DFAS-Cleveland software developer is trained in the use of software development tools. DFAS Human Resources uses a training tracking system to track the completion of training. Supervisors and employees</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry that employees had training and expertise necessary to perform their job responsibilities.</p> <p>Read System Administrator training materials to confirm that they provided the System Administrators with training and expertise necessary to perform their job responsibilities.</p> <p>Inspected a random sample of training records to confirm that the System Administrators had completed the required Level 1 or Level 2 training.</p> <p><u>DFAS-Cleveland</u> Confirmed through inquiry that employees had training and expertise necessary to perform their job responsibilities.</p>	<p><u>DISA DECC-Ogden</u> The System Administrator training was outdated.</p> <p><u>DFAS-Cleveland</u> The technical training program had not been documented. Additionally, there was no documentation available listing all technical training available to staff.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>coordinate annually to prepare Individual Training Plans.</p> <p><u>DFAS-Indianapolis</u> There are training requirements for individuals at a system administrator level. The technical training requirements for the system administrators are broken out by different levels to include: Levels I, II, and III. The supervisor determines the category or level that their system administrators should have.</p>	<p>Confirmed through inquiry of the training manager that a training process was in place for DFAS-Cleveland DDRS staff.</p> <p>Inspected Individual Development Plans to confirm that a plan was on file for DFAS-Cleveland DDRS staff.</p> <p><u>DFAS-Indianapolis</u> Confirmed through inquiry that employees had the training and expertise necessary to perform their job.</p> <p>Confirmed through inquiry of the training manager that a process was in place for training DFAS-Indianapolis DDRS staff.</p> <p>Inspected all six training records to confirm that DDRS DBAs had completed the required Level I, Level II, or Level III training.</p>	<p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>
11	<p>A program is implemented to confirm that upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned Information Assurance responsibilities.</p>	<p><u>DISA DECC-Ogden</u> Each new employee and contactor is provided with a security briefing (they must also sign that they have received this briefing). This briefing is provided annually. New employees and contractors are also required to take the mandatory CD-ROM-based security courses and associated tests to be certified as an ADP Level I or Level II before access is allowed to the systems.</p>	<p><u>DISA DECC-Ogden</u> Read the security awareness briefing used to provide training for new employees at DISA DECC-Ogden.</p> <p>Inspected 17 training records to confirm that employees had completed the necessary security awareness training.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Arlington</u> Each new employee and contractor is provided with a security briefing. They must also sign that they have received this briefing before they are granted access to DDRS. This briefing is posted on the ePortal so that each DFAS user can repeat the briefing annually.</p> <p><u>DFAS-Cleveland</u> Each new DFAS-Cleveland employee and contractor has been provided with a security briefing (they must also sign that they have received this briefing). This briefing was provided online.</p> <p><u>DFAS-Indianapolis</u> Mandatory security awareness training is conducted for all government employees and contractors. A record is kept of each attendee, as well as the specific training and dates attended.</p>	<p><u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Manager the process DFAS-Arlington maintains for security awareness training.</p> <p><u>DFAS-Cleveland</u> Read the Security Awareness Training briefing charts provided by DFAS-Cleveland.</p> <p>Inspected a random sample of 34 DFAS-Cleveland employees to confirm the completion of the necessary security training and that the required signoff signatures had been obtained.</p> <p><u>DFAS-Indianapolis</u> Read the Security Awareness Training briefing charts provided by DFAS-Indianapolis.</p> <p>Inspected all eight training records to confirm that the necessary security training had been completed and that employees had signed off on the training.</p>	<p><u>DFAS-Arlington</u> Although security awareness training was performed, there was no documented process in place to track whether security awareness training was completed.</p> <p><u>DFAS-Cleveland</u> Training materials were outdated and there was no completion notification sent to the Information Assurance Manager or reviewed by the Information Assurance Manager for new employees.</p> <p>Five of 34 Technology Services Organization (TSO) personnel randomly sampled had not completed security awareness training.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
12	Management periodically assesses the appropriateness of security policies and compliance with them.	<p><u>DISA DECC-Ogden</u> Automated SRR scripts are run on each server and reported to the Montgomery SRR database weekly. Each system has a SRR and an Information Security System scan before it is connected to the network. The DISA DECC-Ogden Field Security Office runs periodic SRRs and Information Security System scans. DISA DECC-Ogden conducts reviews of the SSAA, which includes the operation facility environmental risk assessment that is renewed and reviewed annually.</p> <p><u>DFAS-Arlington</u> Every three years, management reviews and assesses the DDRS application security policies and compliance with them during the DITSCAP review process.</p>	<p><u>DISA DECC-Ogden</u> Read the February 2004 Risk Assessment that was performed with the DITSCAP to confirm that risks were periodically assessed.</p> <p>Observed the SRR process to confirm that it occurred and that corrective actions were tracked. Inspected a single SRR performed by DISA DECC-Ogden and inspected the Vulnerability Management System report to confirm findings identified by the SRR process had been addressed.</p> <p>Read the DISA DECC-Ogden SSAA to confirm it had been documented, updated, and appropriately approved.</p> <p><u>DFAS-Arlington</u> Read the Risk Assessment dated June 28, 2002 that was performed during the DITSCAP process to confirm that risks were periodically assessed.</p> <p>Read the DDRS SSAA to confirm it had been documented, updated, and appropriately approved.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
13	Management ensures that corrective actions are effectively implemented.	<p><u>DISA DECC-Ogden</u> Corrective actions are tracked with the Vulnerability Management System and the Information Assurance Vulnerability Alert process to track and maintain system vulnerability status. DISA DECC-Ogden also utilizes Secure Technical Implementation Guides (STIGs), Information Assurance Support Environment, Field Security Office, and weekly SRRs to ensure compliance with DISA policies.</p> <p><u>DFAS-Arlington</u> Management follows up when corrective actions are identified. After each audit an action plan is developed for resolution of any issues. DFAS Information Technology follows up on and tracks the status of CFO audits. DFAS Internal Review follows up on internal audits and tracks issue resolution. The DFAS Acquisition Management Organization is developing a master tracking system covering all Acquisition Management Organization program issues.</p>	<p><u>DISA DECC-Ogden</u> Observed the SRR process to confirm that it occurred and that corrective actions were tracked. Inspected a single SRR performed by DISA DECC-Ogden and inspected the Vulnerability Management System reports to confirm findings identified by the SRR process had been addressed.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry that there was a process in place for tracking findings and corrective actions for DFAS-Arlington.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>
14	A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place.	<p><u>DISA DECC-Ogden</u> Corrective actions are accomplished through the Vulnerability Management System, Information Assurance Vulnerability Alert process to track and maintain system vulnerability status. Additionally, Automated SRR scripts are run on each server and reported to the Montgomery SRR database on a weekly basis. Each system has a</p>	<p><u>DISA DECC-Ogden</u> Read the risk assessment dated February 20, 2004, that was performed with the DITSCAP process to confirm that risks were periodically assessed.</p> <p>Observed the SRR process to confirm that corrective actions were implemented for identified</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>Security Readiness and an Information Security System scan before it is connected to the network. The DISA DECC-Ogden Field Security Office runs periodic SRRs and Information Security System scans. This is covered through the periodic compliance review of UNIX STIG. DISA DECC-Ogden conducts a review of the SSAA, which includes the operation facility environmental risk assessment on an annual basis.</p> <p><u>DFAS-Cleveland</u> A Software Quality Assurance Plan and Software Process Improvement Plan are in place for the systematic identification and mitigation of software vulnerabilities.</p>	<p>SRR findings.</p> <p>Inspected a single SRR and inspected the Vulnerability Management System reports to confirm findings identified by the SRR process had been addressed.</p> <p><u>DFAS-Cleveland</u> Read the DDRS Software Quality Assurance Plan and Software Process Improvement Plan to confirm that they existed and were approved by management.</p> <p>Inspected all six DDRS-AFS releases to confirm that DFAS-Cleveland developers were following their documented policies and procedures.</p>	<p><u>DFAS-Cleveland</u> The following exceptions were noted during our testing of all six DDRS-AFS module releases. We noted the following missing elements: FRR SQA Presence; Function Requirements Review Statement of Agreement; Test Readiness Review and Systems Integration Testing Checklist; Test Readiness Review and Systems Integration Testing Attendee List; Test Readiness Review and Systems Integration Testing Open Item List; Test Readiness Review and Systems Integration Testing Statement of Agreement; Test Readiness Review and Functional Validation Testing Checklist; Test Readiness Review and Functional Validation Testing attendee list; Test Readiness Review and Functional Validation Testing open item list; Test Readiness Review and Functional Validation</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				Testing, Statement of Agreement; Functional Validation Testing Certification Form; Release Implementation Readiness Review Statement of Agreement; Post Implementation Readiness Review Signature; Final Physical Configuration Audit; and Final Functional Configuration Audit.
15	Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation.	<p><u>DISA DECC-Ogden</u> As part of the DITSCAP process, the DISA DECC-Ogden Information Assurance Manager conducts and reviews the SSAA on an annual basis or when there is a major change. Additionally, Automated SRR scripts are run on each server and reported to the Montgomery SRR database on a weekly basis. Each system has a SRR and an Information Security System scan before it is connected to the network. The DISA Field Security Office runs periodic SRRs and Information Security System scans.</p> <p><u>DFAS-Arlington</u> The Information Assurance Officer reviews all system changes for Information Assurance impact prior to approval by the DDRS Configuration</p>	<p><u>DISA DECC-Ogden</u> Read the risk assessment dated February 20, 2004, that was performed with the DITSCAP process to confirm that risks were periodically assessed.</p> <p>Confirmed through inquiry with the Information Assurance Manager that the SSAA was updated on an annual basis.</p> <p>Observed the SRR process to confirm that corrective actions were implemented for identified SRR findings.</p> <p>Inspected a single SRR and the Vulnerability Management System reports to confirm findings identified by the SRR process had been addressed.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry that the Information Assurance Manager was involved in the Configuration Change Board</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>Change Board. The DDRS application security risks are randomly sampled and analyzed every three years. These risks are reported to DFAS Information Assurance management, and are considered for accreditation and re-accreditation every three years.</p>	<p>and assessed the DDRS changes for their impact on information assurance.</p> <p>Confirmed through inquiry with the Information Assurance Manager that the SSAA was updated every three years. Read the DDRS SSAA to confirm it had been documented, updated, and appropriately approved.</p>	
16	<p>A DoD reference document constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled Information Technology products.</p>	<p><u>DISA DECC-Ogden</u> As part of the DITSCAP process, the DISA DECC-Ogden Information Assurance Manager conducts and reviews the SSAA on an annual basis or when there is a major change. Additionally, Automated SRR scripts are run on each server and reported to the Montgomery SRR database on a weekly basis. Each system has a SRR and an Information Security System scan before it is connected to the network. The DISA Field Security Office runs periodic SRRs and Information Security System scans. This is covered through the periodic compliance review of Unix Security Technical Implementation Guide.</p>	<p><u>DISA DECC-Ogden</u> Read the risk assessment dated February 20, 2004, that was performed with the DITSCAP to confirm that risks were periodically assessed.</p> <p>Confirmed through inquiry with the Information Assurance Manager that the SSAA was updated on an annual basis.</p> <p>Observed the SRR process to confirm that corrective actions were implemented for identified SRR findings.</p> <p>Inspected a single SRR and the Vulnerability Management System reports to confirm findings identified by the SRR process had been addressed. Read the UNIX STIG and the DISA DECC-Ogden SSAA to confirm that they constituted the</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			primary source configuration or implementation guidance for the deployment of newly acquired IA and IA-enabled products.	
	<i>Access Controls</i>			
17	Resource classifications and related criteria have been established.	<p><u>DFAS-Arlington</u> DoD Instruction 8500.2 states (paraphrased): It is public information if it has been formally reviewed and approved for public release in accordance with DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996. It is classified information if it has been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Only an Originating Classification Authority has the authority to classify information and DFAS does not have that authority. Therefore, DFAS treats its information as being classified only when it is marked as such or when compiling information as indicated by an existing classification guide originating from outside of DFAS. None of the data contained within DDRS is classified or cleared for public release; therefore DDRS data is considered sensitive but unclassified.</p>	<p><u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Officer that DDRS data had been classified as sensitive but unclassified.</p> <p>Read the SSAA to confirm that data had been classified as sensitive but unclassified.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
18	Owners have classified resources.	<p><u>DFAS-Arlington</u> DDRS does not contain or store classified data. Final reports produced by DDRS are often reviewed and approved for public release, but this process is performed outside DDRS. Financial Information processed and stored by DDRS is processed and stored as Sensitive data in accordance with the definition found in DoD 5200.1-R, "Information Security Program," January 1997. Security audit reports displaying user names are marked "For Official Use Only" in accordance with DoD guidance on Privacy Act data.</p>	<p><u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Officer that DDRS data had been classified as Sensitive But Unclassified.</p> <p>Read the SSAA to confirm that data had been assigned a classification level of Sensitive But Unclassified.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>
19	Resource owners have identified authorized users and their access authorized.	<p><u>DISA DECC-Ogden</u> There are three levels of privileged accounts for the DDRS Operating System. These levels are based on need-to-know access rules. All users must fill out the SAAR form and have a Government official sign the form, confirming need-to-know access.</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of the DDRS System Administrator the process for obtaining an administrator account on the DDRS Operating System.</p> <p>Inspected all nine SAAR forms to confirm that a form was on file for all System Administrators with access to the DDRS Operating System.</p>	<p><u>DISA DECC-Ogden</u> Seven of nine SAAR forms inspected did not have the signature of the Information Assurance Officer on the SAAR form.</p> <p>One System Administrator did not have a SAAR form on file. Additionally, access had not been removed for that user in a timely manner. This user's access was subsequently deleted because he no longer required access to DDRS.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Arlington</u> The DDRS Functional Data Owners identify and establish the authorized DDRS users by signing the SAAR form. The database administrators will not accept a new user request unless it is from a Functional Data Owner.</p> <p><u>DFAS-Cleveland</u> Cleveland Management has identified and authorized Configuration Management Information System (CMIS), Program Version Control System (PVCS) and Oracle Versioning users and their access has been documented and approved. CMIS is used by PMO staff to track system changes made to DDRS.</p>	<p><u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Officer the process for obtaining a user account on DDRS.</p> <p>Inspected all 18 SAAR forms to confirm that a form was on file for the DDRS PMO staff with access to DDRS.</p> <p>Inspected all 22 access forms to confirm that a form was on file for PMO staff with access to the CMIS.</p> <p><u>DFAS-Cleveland</u> Confirmed the process for recording access to the CMIS, the PVCS, and the Oracle Versioning application through inquiry of the following DDRS personnel: DDRS Configuration Manager; PVCS; Configuration Manager; and DDRS Budgetary Module Team Lead.</p> <p>Inspected CMIS access forms to confirm that a form was on file for the 33 DDRS development staff with access to the CMIS.</p> <p>Inspected all 31 Repository User Access Forms to confirm that a form was on file for the DDRS development staff with access to the Oracle Versioning System.</p>	<p><u>DFAS-Arlington</u> Three of 18 SAAR forms did not document justification for access; another three of 18 did not document type of system access.</p> <p>One of 22 CMIS PMO users had access to roles that were not required for his duties. Seven of 22 CMIS PMO users were former DDRS PMO staff, but their access to CMIS had not been terminated.</p> <p><u>DFAS-Cleveland</u> There were no forms used to track PVCS access.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Indianapolis</u> DDRS Database Administrator (DBA) access to production servers is documented through a SAAR form. These forms are maintained by DISA DECC-Ogden.</p>	<p>Requested access forms to confirm that a form was on file for DDRS development staff with access to the PVCS.</p> <p><u>DFAS-Indianapolis</u> Inquired of the DDRS Project Manager and the lead DBA of the process for granting DBAs access to DDRS.</p> <p>Inspected all six SAAR forms to confirm that a form was on file for the DBAs with access to DDRS.</p> <p>Inquired of the end user account administrator regarding DDRS end user account creation, modification, deletion, and password reset process.</p>	<p><u>DFAS-Indianapolis</u> One of six SAAR forms for DBAs did not have the justification for access completed on the SAAR form.</p> <p>None of the six SAAR forms inspected for DBAs had the signatures of the Functional Data Owner and Information Assurance Officer.</p> <p>One of six DBAs approved his own SAAR form.</p>
20	Emergency and temporary access authorization is controlled.	<p><u>DISA DECC-Ogden</u> DISA DECC-Ogden has not issued emergency and temporary access authorization to the DDRS Operating System over the past year. If a vendor needs to make a change to the Operating System, the DDRS system administrators will complete the required actions with the vendor present.</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of the System Administrator the process for obtaining an administrator account on the DDRS Operating System.</p> <p>Confirmed with the System Administrator that the vendor was present when changes were made.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Arlington</u> If an emergency or temporary account is needed, the individual must complete the user access request SAAR form.</p> <p>Emergency or temporary access is controlled using the same controls as normal access, but with a higher priority. If a non-user has an urgent DDRS data request, they must ask an authorized DDRS user to produce it for them.</p> <p><u>DFAS-Cleveland</u> DFAS-Cleveland does not grant emergency or temporary access to the PVCS, Oracle Versioning application, and CMIS.</p> <p><u>DFAS-Indianapolis</u> Emergency access for a new account is rarely, if ever granted. There are some emergency resets of existing account passwords that are handled by the Technology Services Organization Mid-tier Support Team. Temporary access is authorized for limited capability on demonstrations and specific software for a limited amount of time. This access is with government personnel supervising or assisting for the period of the demonstration only.</p>	<p><u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Officer the process for obtaining an emergency or temporary DDRS administrator account</p> <p><u>DFAS-Cleveland</u> Confirmed through inquiry of DDRS Configuration Manager, PVCS Configuration Manager, and DDRS Budgetary Module Team Lead the process for recording access to the CMIS, the PVCS, and the Oracle Versioning application.</p> <p><u>DFAS-Indianapolis</u> Inquired of the DDRS Project Manager and the lead DBA of the process for obtaining emergency or temporary DBA access to DDRS.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p> <p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
21	Owners determine disposition and sharing of data.	<u>DFAS-Arlington</u> Access to and sharing of data within DDRS is controlled by user roles and work areas. Work areas restrict user access to specific data subsets based on their organizational responsibility. Functional Data Owners at the DDRS PMO are responsible for maintaining the user roles and work areas within DDRS in accordance with approved SAAR forms.	<u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Officer that DDRS data had been classified as sensitive but unclassified and confirmed the lack of automated system interfaces. Read the SSAA to confirm that data had been assigned a classification level of sensitive but unclassified and that there were no automated system interfaces.	<u>DFAS-Arlington</u> No relevant exceptions noted.
22	Adequate physical security controls have been implemented.	<u>DISA DECC-Ogden</u> Each individual must first gain access to Hill Air Force Base, UT. Then the individual has to pass through a guard at the front desk where proper identification must be displayed to allow the individual access to the Data Center. To enter the Data Center, an individual must have a swipe badge with the appropriate level of access.	<u>DISA DECC-Ogden</u> Observed the physical safeguards in place for DISA DECC-Ogden. Observed that facility penetration testing processes were in place that included periodic, unannounced attempts to penetrate key computing facilities. Additionally, observed that every physical access point that displayed sensitive information or unclassified information that had not been cleared for release was controlled during business hours and guarded or locked during non-business hours.	<u>DISA DECC-Ogden</u> No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Arlington</u> Access to DFAS-Arlington is controlled using building identification badges such as the Pentagon or CM3 badge. Security guards at the entrance enforce the use of badges.</p> <p><u>DFAS-Cleveland</u> DFAS-Cleveland is a tenant of a government-shared public building employing security guards and metal detectors at the entrance.</p> <p><u>DFAS-Indianapolis</u> General Services Administration and Homeland Security have complete control over facility access by all individuals. A metal detector is employed to screen all individuals and their baggage on entering the facility.</p>	<p><u>DFAS-Arlington</u> Observed the physical safeguards in place for DFAS-Arlington.</p> <p>Interviewed building security personnel to confirm that appropriate physical security controls had been implemented.</p> <p>Inspected the Access Procedures Crystal Mall policies in place for controlling access to DFAS-Arlington.</p> <p><u>DFAS-Cleveland</u> Observed the physical safeguards in place for DFAS-Cleveland.</p> <p>Interviewed building security personnel to confirm that appropriate physical security controls had been implemented.</p> <p><u>DFAS-Indianapolis</u> Observed the physical safeguards in place for DFAS-Indianapolis.</p> <p>Interviewed building security personnel to confirm that required physical security controls had been implemented.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p> <p><u>DFAS-Cleveland</u> There were no documented DFAS-specific visitor policies in place and there were inadequate physical security controls to restrict access to the DDRS developer workspace.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
23	Physical safeguards have been established that are commensurate with the risks of physical damage or access.	<p><u>DISA DECC-Ogden</u> Each individual must first gain access to Hill Air Force Base, UT. During normal duty hours, visitors are controlled by a person posted in the lobby. Entry is also controlled for computer rooms. Building 891 is a one-story structure. There are nine entry and exit points. All are locked or controlled. The facility contains 142,792 square feet. The building uses commercial power. In the event of a commercial power failure, the building can operate by using the Uninterruptible Power Source, supplemented by backup generators, which ensures continued operation. The facility has 1,200 tons cooling capacity.</p>	<p><u>DISA DECC-Ogden</u> Confirmed that facility penetration testing processes were in place that included periodic, unannounced attempts to penetrate key computing facilities. Further, every physical access point that displayed sensitive but unclassified information that had not been cleared for release was controlled during business hours and guarded or locked during non-business hours.</p> <p>Observed that the DDRS Data Center was protected by fire suppression and these prevention devices were installed and working. Observed that there was an Uninterruptible Power Source and that the cooling system was maintained.</p> <p>Confirmed that DISA DECC-Ogden contained a master power override switch to stop the power flow to Information Technology equipment and that the master power override switch was optimally located at the entrance of the data center and clearly labeled.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
24	Visitors are controlled.	<p><u>DISA DECC-Ogden</u> Each visitor to the DISA DECC-Ogden facility must first gain access to Hill Air Force Base, UT. Then the visitor must pass by a guard at the front desk where the visitor must sign the visitor control log. Next, an employee of the Data Center must sign the visitor control log as escort for the visitor. Additionally, the visitor must be issued and wear a temporary badge at all times while inside the Data Center. Finally, when the visitor exits the facility, the visitor's badge must be returned to the front desk.</p> <p><u>DFAS-Arlington</u> Visitors to DFAS-Arlington must have a visitor's badge and must have an escort depending on the type of identification provided to the security guards.</p> <p><u>DFAS-Cleveland</u> Visitors to DFAS-Cleveland must have a DoD Identification Badge or must be escorted.</p>	<p><u>DISA DECC-Ogden</u> Read the visitor policy and procedure for DISA DECC-Ogden to confirm they were documented. Observed the visitor check-in and check-out process for DISA DECC-Ogden.</p> <p>Confirmed through inquiry and observation that visitor access to DoD information was determined by both its classification and user need-to-know.</p> <p>Inspected 45 visitor request letters to verify they existed and were maintained.</p> <p><u>DFAS-Arlington</u> Read the visitor policy and procedure for DFAS-Arlington to confirm they were documented. Observed the visitor check-in and check-out process for DFAS-Arlington. Confirmed through inquiry and observation that visitor access to DoD information was determined by its classification and user need-to-know.</p> <p><u>DFAS-Cleveland</u> Requested the visitor policy and procedure for DFAS-Cleveland to confirm they were documented. Observed the</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p> <p><u>DFAS-Cleveland</u> Five of 12 visitor request letters were missing. Additionally, there was not a DFAS specific visitor log and individuals were only</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Indianapolis</u> A valid ID must be displayed and presented to the guard at each entry of the building. If a person has no valid identification, they are directed to the security office for issuance of a visitor badge. The visitor badge must be signed for by someone in the office being visited and the visitor must be escorted by that individual.</p>	<p>visitor check in and check out process for DFAS-Cleveland.</p> <p>Confirmed through inquiry and observation that visitor access to DoD information was determined by both its classification and user need-to-know.</p> <p>Requested all 12 visitor request letters to verify that they existed and were being retained.</p> <p><u>DFAS-Indianapolis</u> Read the visitor policy and procedure for DFAS-Indianapolis to confirm they were documented. Observed the visitor check in and check out process for DFAS-Indianapolis.</p> <p>Confirmed through inquiry and observation that visitor access to DoD information is determined by its classification of the data and user need-to-know.</p> <p>Inspected visitor sign-in sheets to verify that they were being maintained.</p>	<p>required to sign a general facility visitor's log when the individual did not have a photo ID.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>
25	Adequate logical access controls have been implemented at the application and Operating System layer.	<p><u>DISA DECC-Ogden</u> To gain logical access to the DDRS Operating System a user must have a valid User ID and password.</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of the DDRS System Administrator the process for obtaining an administrator account on the DDRS Operating System.</p>	<p><u>DISA DECC-Ogden</u> Seven of nine SAAR forms inspected did not have the signature of the Information Assurance Officer on the SAAR form.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Arlington</u> To gain access to the DFAS-Arlington Network, users must use a DoD Common Access Card and pin number. Additionally, a user must have an authorized User ID and password to gain access to the DDRS application.</p> <p><u>DFAS-Cleveland</u> User authentication is required for access to user workstations, and an additional authentication is required to access the software development tools PVCS, CMIS, and Oracle versioning.</p>	<p>Inspected all nine SAAR forms to confirm that a form was on file for all System Administrators with access to the DDRS Operating System.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Officer the process for obtaining a user account on DDRS. Inspected all 18 SAAR forms to confirm that a form was on file for the DDRS PMO staff with access to DDRS.</p> <p>Inspected all 22 access forms to confirm that a form was on file for PMO staff with access to the CMIS.</p> <p><u>DFAS-Cleveland</u> Confirmed through inquiry of DDRS Configuration Manager, PVCS Configuration Manager, and DDRS Budgetary Module Team Lead the process for recording access to the CMIS, the PVCS, and the Oracle Versioning application.</p> <p>Inspected CMIS access forms to confirm that a form was on file for the 33 DDRS development staff with access to the CMIS.</p>	<p>One System Administrator did not have a SAAR form on file. Additionally, access had not been removed for that user in a timely manner. This user's access was subsequently deleted because he no longer required access to DDRS.</p> <p><u>DFAS-Arlington</u> Three of 18 SAAR forms did not document justification for access; another three of 18 did not document type of system access. One of 22 CMIS PMO users had access to roles that were not required for his duties.</p> <p>Seven of 22 CMIS PMO users were former DDRS PMO staff, but their access to CMIS had not been terminated.</p> <p><u>DFAS-Cleveland</u> There were no forms used to track PVCS access.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Indianapolis</u> Technology Services Organization access to all systems is controlled either through the Form 1018 (Mid-tier access request) or, for DISA platforms or applications, a SAAR form must be completed and signed by the Functional Data Owner and supervisor and the Terminal Area Security Officer for access.</p>	<p>Inspected all 31 6i Repository User Access Forms for DFAS-Cleveland DDRS staff members to confirm that a form was on file for the DDRS development staff with access to the Oracle Versioning System.</p> <p>Requested access forms to confirm that a form was on file for DDRS development staff with access to the PVCS.</p> <p><u>DFAS-Indianapolis</u> Inquired of the DDRS Project Manager and the lead DBA on the process used for granting DBAs access to DDRS.</p> <p>Inspected all six SAAR forms to confirm that a form was on file for DBAs with access to DDRS.</p> <p>Inquired of the end user account administrator regarding DDRS end user account creation, modification, deletion, and password reset process.</p>	<p><u>DFAS-Indianapolis</u> One of six SAAR forms for DBAs did not have the justification for access completed on the SAAR form.</p> <p>None of the six SAAR forms inspected for DBAs had the signatures of the Functional Data Owner and Information Assurance Officer.</p> <p>One of six DBAs approved his own SAAR form.</p>
26	<p>Passwords, tokens, or other devices are used to identify and authenticate users.</p>	<p><u>DISA DECC-Ogden</u> To gain logical access to the DDRS Operating System, a user must have a correct User ID and password. Password parameters are as follows: -Password must be at least 8 characters in length, and -Password must contain two of the</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of the DDRS System Administrator that passwords were used to authenticate Operating System users.</p>	<p><u>DISA DECC-Ogden</u> Password complexity could not be enforced on the Solaris platform, due to Operating System limitations. Solaris was the Operating System used for DDRS.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>following three: at least one upper case, a number, or a special character (use @, #, \$, or _).</p> <p><u>DFAS-Arlington</u> A user ID and Password is required to access DDRS.</p> <p><u>DFAS-Indianapolis</u> Workstation authentication is controlled using Common Access Card smartcard Public Key Infrastructure tokens. All developer tools require a login using a user ID and password unique for the individual.</p>	<p>Reviewed password setting within Solaris for compliance with Security Technical Implementation Guide requirements.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry of the DDRS Information Assurance Officer that passwords were required to authenticate DDRS end users.</p> <p>Reviewed DDRS password settings to confirm compliance with DoD Instruction 8500.2 requirements.</p> <p><u>DFAS-Indianapolis</u> Confirmed through inquiry of the end user account administrator the process for password resets and new user password creation.</p> <p>Confirmed through inquiry of the end user account administrator that passwords were changed from default password settings.</p>	<p><u>DFAS-Arlington</u> DDRS did not log users out after a specified period of inactivity and users were not automatically prompted to change the initial generic password that they were issued.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>
27	Access paths are identified as part of a risk analysis and documented in an access path diagram.	<p><u>DISA DECC-Ogden</u> The vast amount of information stored, processed, and transferred by the Automated Information systems make them a lucrative target of a diverse, worldwide threat intent on compromise of data, corruption of data, and</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of the Lead Firewall Technician and Communications Chief that an access path diagram existed and was current.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>disruption of service, or actual physical destruction. The threat is diverse in source, motivation, sophistication, technique, and time. It includes hackers fascinated by technical challenge, foreign governments with military and economic interest, disgruntled employees, and unintentional software errors. While the threat is predominantly in the operational phase of the system life cycle, it is present throughout the system development and system sustainment phases. Automated Information systems frequently serve users through direct and networked dial-up connections. A logical network diagram has been developed which documents the access paths for DDRS.</p> <p><u>DFAS-Arlington</u> Access paths are identified and diagrammed in the DDRS SSAA.</p>	<p>Read network diagrams to confirm that they were accurate and current.</p> <p>Read the DISA DECC-Ogden SSAA to confirm that logical access paths were identified and approved by management.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Manager that an access path diagram existed and was current.</p> <p>Read the DDRS SSAA to confirm that logical access paths were identified and approved by management.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>
28	Access is restricted to data files and software programs.	<p><u>DISA DECC-Ogden</u> DISA DECC-Ogden creates user IDs and passwords as well as access levels as documented in the SAAR form.</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of the DDRS System Administrator the process for obtaining an administrator account on the DDRS Operating System.</p>	<p><u>DISA DECC-Ogden</u> Seven of nine SAAR forms inspected did not have the signature of the Information Assurance Officer on the SAAR form.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Arlington</u> Access to DDRS data and to any DDRS program is restricted by using user authentication. Access is restricted by the Functional Data Owners. Individuals must have a requirement or need-to-know to access a specific application. The access for each application or database is granted by Functional Data Owners.</p> <p><u>DFAS-Cleveland</u> Configuration Control and Versioning control systems are in place throughout the development and implementation process to ensure access control. These systems are CMIS, PVCS, and Oracle Designer.</p>	<p>Inspected all nine SAAR forms to confirm that a form was on file for all System Administrators with access to the DDRS Operating System.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Officer the process for obtaining a user account on DDRS.</p> <p>Inspected all 18 SAAR forms to confirm that a form was on file for the DDRS PMO staff with access to DDRS.</p> <p>Inspected all 22 access forms to confirm that a form was on file for PMO staff with access to the CMIS.</p> <p><u>DFAS-Cleveland</u> Confirmed the process for recording access to the CMIS, the PVCS, and the Oracle Versioning application through inquiry of the following DDRS personnel: DDRS Configuration Manager; PVCS Configuration Manager; and DDRS Budgetary Module Team Lead.</p>	<p>One System Administrator did not have a SAAR form on file. Additionally, access had not been removed for that user in a timely manner. This user's access was subsequently deleted because he no longer required access to DDRS.</p> <p><u>DFAS-Arlington</u> Three of 18 SAAR forms did not document justification for access; another three of 18 did not document type of system access.</p> <p>One of 22 CMIS PMO users had access to roles that were not required for his duties.</p> <p>Seven of 22 CMIS PMO users were former DDRS PMO staff, but their access to CMIS had not been terminated.</p> <p><u>DFAS-Cleveland</u> There were no forms used to track PVCS access.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Indianapolis</u> DBA Access is documented on the DISA Form 41 which is maintained by DISA Ogden and access is restricted to development tools such as PVCS, Oracle Versioning, and CMIS.</p>	<p>Inspected CMIS access forms to confirm that a form was on file for the 33 DDRS development staff with access to the CMIS.</p> <p>Inspected all 31 6i Repository User Access Forms on DFAS-Cleveland staff members to confirm that a form was on file for the DDRS development staff with access to the Oracle Versioning System.</p> <p>Requested access forms to confirm that a form was on file for DDRS development staff with access to the PVCS.</p> <p><u>DFAS-Indianapolis</u> Inquired of the DDRS Project Manager and the lead DBA of the process for granting the DBA access to DDRS.</p> <p>Inspected all six SAAR forms to confirm that a form was on file for the DBAs with access to DDRS.</p> <p>Inquired of the end user account administrator regarding DDRS end user account creation, modification, deletion, and password reset process for DDRS.</p>	<p><u>DFAS-Indianapolis</u> One of six SAAR forms for DBAs did not have the justification for access completed on the SAAR form.</p> <p>None of the six SAAR forms inspected for DBAs had the signatures of the Functional Data Owner and Information Assurance Officer.</p> <p>One of six DBAs approved his own SAAR form.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
29	<p>Access settings have been implemented in accordance with the access authorizations established by the resource owners.</p>	<p><u>DISA DECC-Ogden</u> Ogden creates user IDs and passwords as well as access levels as documented in the SAAR form.</p> <p><u>DFAS-Arlington</u> Each DDRS user has access restricted to specific data sets and functional roles as established by the Functional Data Owners.</p> <p><u>DFAS-Cleveland</u> Configuration Control and Versioning control systems are in place throughout the development and implementation process to ensure access control. These systems are CMIS, PVCS, and Oracle Designer.</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of the DDRS System Administrator the process for obtaining an administrator account on the DDRS Operating System.</p> <p>Inspected all nine SAAR forms to confirm that a form was on file for System Administrators with access to the DDRS Operating System.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Officer the process for obtaining a user account on DDRS.</p> <p>Inspected all 18 SAAR forms to confirm that a form was on file for the DDRS PMO staff with access to DDRS.</p> <p>Inspected all 22 CMIS access forms to confirm that an access form was on file for PMO staff having access to the CMIS.</p> <p><u>DFAS-Cleveland</u> Confirmed the process for recording access to the CMIS, the PVCS, and the Oracle Versioning application through inquiry of the following DDRS personnel: DDRS Configuration Manager; PVCS Configuration</p>	<p><u>DISA DECC-Ogden</u> Seven of nine SAAR forms did not have the signature of the Information Assurance Officer.</p> <p>One out of nine users did not have a SAAR form on file because the user no longer required access. However, the access had not been terminated. The user's access was terminated after our testing.</p> <p><u>DFAS-Arlington</u> Three of 18 SAAR forms did not document justification for access, and another three did not document type of system access.</p> <p>One of 22 CMIS PMO users had access to roles that were not required for his duties.</p> <p>Seven of 22 CMIS PMO users were former DDRS PMO staff, but their access to CMIS had not been terminated.</p> <p><u>DFAS-Cleveland</u> There were no forms used to track PVCS access.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Indianapolis</u> DBA access is documented on the DISA Form 41 which is maintained by DISA DECC-Ogden and access is restricted to development tools such as PVCS, Oracle Versioning, and CMIS.</p>	<p>Manager; and DDRS Budgetary Module Team Lead.</p> <p>Inspected CMIS access forms to confirm that a form was on file for the 33 DDRS development staff with access to the CMIS.</p> <p>Inspected all 31 6i Repository User Access Forms on DFAS-Cleveland DDRS staff members to confirm that a form was on file for the DDRS development staff with access to the Oracle Versioning System.</p> <p>Requested access forms to confirm that a form was on file for DDRS development staff with access to the PVCS.</p> <p><u>DFAS-Indianapolis</u> Inquired of the DDRS Project Manager and the lead DBA of the process for granting the DBA access to DDRS.</p> <p>Inspected all six SAAR forms to confirm that a form was on file for the DDRS DBAs with access to DDRS.</p> <p>Inquired of the end user account administrator regarding DDRS end user account creation, modification, deletion, and password reset process.</p>	<p><u>DFAS-Indianapolis</u> One of six SAAR forms for DBAs did not have the justification for access completed on the SAAR form.</p> <p>None of the six SAAR forms inspected for DBAs had the signature of the Functional Data Owner and the Information Assurance Officer.</p> <p>One of six DBA approved his own SAAR form.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
30	Telecommunications controls are properly implemented in accordance with authorizations that have been granted.	<p><u>DISA DECC-Ogden</u> Virtual Private Network (VPN) and dial-in are the telecommunications methods used in DDRS. DISA DECC-Ogden uses software called Radius and Tac-X to ensure there are secure telecommunication capabilities. If VPN or dial-up access is needed then, the end user must fill out the DoD Form 41 or SAAR form.</p> <p><u>DFAS-Arlington</u> VPN and dial-in are the telecommunications methods used by DFAS for remote DDRS access. A DFAS user requiring remote access must obtain a DFAS laptop computer equipped with VPN or DFAS Internet Service Provider software. If VPN or DFAS Internet Service Provider access is needed, then the end user must fill out the DFAS Internet Service Provider request form in addition to their own DoD Form 2875 for DDRS access.</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of the Lead Firewall Technician and Communications Chief that VPN and dial-in accounts were maintained at DISA DECC-Ogden. Verified that the VPN was noted on the network diagrams.</p> <p>Performed network monitoring testing to test for unauthorized network connections.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Officer that VPN and dial-in accounts were maintained at the DFAS-wide level and were not specific to DDRS.</p>	<p><u>DISA DECC-Ogden</u> There were connection attempts from unauthorized hosts to the DDRS database server. These attempts did not appear to be successful.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>
31	Procedures are in place to clear sensitive information and software from computers, disks, and other equipment or media when they are disposed of or transferred to another use.	<p><u>DISA DECC-Ogden</u> The guidelines provided by DoD are followed for the destruction of platters and the certification of destruction is completed by the Facilities Office personnel responsible for the disposition of the drives (either bad or upgraded and purchased and leased.)</p>	<p><u>DISA DECC-Ogden</u> Read the Disposition of Unclassified DoD Computer Hard Drives policy used by DISA DECC-Ogden. Confirmed policy was being used.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Arlington</u> The DFAS Desktop Management Initiative team removes computers and disks that are to be disposed of or converted to another use from the work areas. They then re-image the machines before re-using or disposing of them.</p> <p><u>DFAS-Cleveland</u> DoD approved utility called "Wipe Drive" is run on each PC. The utility can be set to achieve the level of security required.</p> <p><u>DFAS-Indianapolis</u> DFAS-Indianapolis follows DoD requirements for clearing data from computers and other media.</p>	<p>Inspected a sample of Certification of Hard Drive Disposition forms used to track the completion of cleared hard drives at DISA DECC-Ogden.</p> <p><u>DFAS-Arlington</u> Read the Hardware Excising policy used by DFAS-Arlington. Confirmed policy was being used.</p> <p>Inspected the log of the wiped and destroyed devices.</p> <p><u>DFAS-Cleveland</u> Read the Disposition of Unclassified DoD Computer Hard Drives policy used by DFAS-Cleveland. Confirmed that the policy was being used.</p> <p>Inspected the log of the wiped and destroyed devices.</p> <p><u>DFAS-Indianapolis</u> Read the DoD Computer Hard Drives Prior To Disposal policy used by DFAS-Indianapolis.</p> <p>Confirmed that the policy was being used.</p> <p>Inspected a sample of Certification of Hard Drive Disposition forms, used to track the completion of cleared hard drives at DFAS-Indianapolis.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p> <p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
32	Audit trails are maintained at the application, Operating System and database layers.	<p><u>DISA DECC-Ogden</u> Operating System audit files are periodically moved to an audit server located at DISA DECC-Ogden. The audit files are then burned to CD and stored on site for one year. After one year, the CDs are destroyed.</p> <p>Operating System Audit files are maintained per UNIX STIG requirements. Audit files are stored on tape on site.</p> <p><u>DFAS-Cleveland</u> DFAS-Cleveland develops and implements audit trails at the DDRS application level.</p> <p><u>DFAS-Indianapolis</u> DFAS-Indianapolis maintains database alert and listener logs and other database related logs. The logs are reviewed by the DBAs on a daily basis. Operating System audit files are maintained per UNIX STIG requirements. Audit files are stored on tape on site.</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of an IT Specialist that audit trails were created and reviewed for the DDRS Operating System.</p> <p><u>DFAS-Cleveland</u> Inquired of the DDRS developers to confirm the existence of audit trails for DDRS.</p> <p>Inspected a random sample of audit trails to confirm the audit trails existed.</p> <p><u>DFAS-Indianapolis</u> Inquired of the DBAs to confirm audit trails existed for DDRS.</p> <p>Inspected a random sample of audit trails to confirm the audit trails existed.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>
33	The contents of audit trails are protected against unauthorized access, modification or deletion.	<p><u>DISA DECC-Ogden</u> Audit files are maintained per UNIX STIG requirements. Audit files are stored on tape on site.</p>	<p><u>DISA DECC-Ogden</u> Verified through observation the read and write access to the audit logs for the DDRS Operating System was restricted</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Cleveland</u> The application audit trails are inherently archived at the table level and backed up and archived with the database. The audit trails are maintained as read-only.</p> <p><u>DFAS-Indianapolis</u> Permissions on the audit files are restricted to the DBAs only. DISA System Administrators also can view these files, but only on an "as needed" basis.</p>	<p>to root-privileged users.</p> <p><u>DFAS-Cleveland</u> Through observation, verified the read and write access to the audit logs for the DDRS application were restricted to DBA-privileged users.</p> <p><u>DFAS-Indianapolis</u> Through observation, verified the read and write access to the audit logs for the DDRS application and database were restricted to DBA-privileged users.</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p> <p><u>DFAS-Indianapolis</u> DFAS-Indianapolis was unable to provide a system-generated listing of individuals with read or write access to the application and database audit trails.</p>
34	Tools are available for the review of audit records and for report generation from audit records.	<p><u>DISA DECC-Ogden</u> HP Audit Tools are used to view audit records.</p> <p><u>DFAS-Arlington</u> The DDRS software has online report generation capability for each audit trail.</p> <p><u>DFAS-Cleveland</u> Oracle Enterprise Manager is used to generate audit trail reports at the application level for DCM and AFS Modules. For the DDRS-Budgetary Module, Web Graphical Interface is used for the generation of audit reports.</p>	<p><u>DISA DECC-Ogden</u> Inspected the tools available to DISA DECC-Ogden personnel and confirmed that they supported the security function.</p> <p><u>DFAS-Arlington</u> Inspected the tools available to DFAS-Arlington personnel and confirmed that they supported the security function.</p> <p><u>DFAS-Cleveland</u> Inspected the tools available to DFAS-Cleveland personnel and confirmed that they supported the development function.</p>	<p><u>DISA DECC-Ogden</u> DISA DECC-Ogden did not proactively monitor or review Operating System audit trails.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p> <p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<u>DFAS-Indianapolis</u> Scripts are written that can extract the information from the audit logs to report on activity.	<u>DFAS-Indianapolis</u> Inquired of DBAs that automated tools were available for viewing audit trails. Inspected scripts used for viewing audit trails at the database level.	<u>DFAS-Indianapolis</u> No relevant exceptions noted.
35	Actual or attempted unauthorized, unusual, or sensitive network access is monitored.	<u>DISA DECC-Ogden</u> Authorized and unauthorized network access is monitored through TCP Wrapper and Klaxon or Banshee. Host based-Intrusion Detection System, Symantec Enterprise Security Manager, and Intruder Alert are installed on all UNIX servers.	<u>DISA DECC-Ogden</u> Inquired of the System Security Administrator to confirm that unauthorized, unusual, or sensitive access was monitored . Performed network monitoring using the Securify tool to test whether DDRS interfaces were monitored with the Intruder Alert server.	<u>DISA DECC-Ogden</u> No relevant exceptions noted.
36	Suspicious or irregular access activity is investigated and appropriate action taken.	<u>DISA DECC-Ogden</u> When suspicious activity is detected, initial investigation is performed. If deemed an actual event, the Continental United States Regional Computer Emergency Response Team is notified and action is taken as required.	<u>DISA DECC-Ogden</u> Inquired of the Security Administrator to confirm that suspicious or irregular access activity was investigated and appropriate actions were taken.	<u>DISA DECC-Ogden</u> No relevant exceptions noted.
37	The acquisition, development, and use of mobile code to be deployed in DoD systems meet current guidelines, standards and regulations.	<u>DFAS-Arlington</u> Mobile code used by DDRS consists of Java Applets running within the Sun Java Virtual Machine or under Oracle J-Initiator. DoD policy defines these technologies as “Category 2 Mobile Code” which must be either used within an enclave or be digitally signed. If an applet is obtained from a trusted source	<u>DFAS-Arlington</u> Inquired of the Information Assurance Officer to confirm that the acquisition, development, and use of mobile code to be deployed in DoD systems met current guidelines, standards, and regulations.	<u>DFAS-Arlington</u> No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>over an assured channel, or if it is signed with a DoD-approved Public Key Information certificate, then the DoD mobile policy says users may execute it. Providing an applet over an assured channel that provides source authentication, such as Secure Socket Layer or Transport Layer Security, is a Policy-compliant way to provide an applet in a trusted fashion. DDRS mobile code components are transmitted using a Secure Socket Layer channel, which is digitally signed and authenticated with a DoD issued Public Key Information certificate.</p> <p><u>DFAS-Cleveland</u> By definition, mobile code is software obtained from remote systems outside the enclave boundary, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. Therefore, this item is not applicable to DDRS releases.</p>	<p><u>DFAS-Cleveland</u> Inquired with appropriate personnel to confirm that the acquisition, development, and use of mobile code to be deployed in DoD systems met current guidelines, standards, and regulations.</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p>
38	All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates.	<p><u>DISA DECC-Ogden</u> All workstations and servers use antivirus software.</p>	<p><u>DISA DECC-Ogden</u> Observed that servers, workstations, and mobile computing devices implemented virus protection that included a capability for automatic updates for all DDRS locations.</p> <p>Inspected a screen print as evidence that these settings had been configured.</p>	<p><u>DISA DECC-Ogden</u> The test results have been removed from the SAS 70 Report due to the sensitivity of the information contained in the test results.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Arlington</u> All workstations and servers at DFAS-Arlington use antivirus software, which has an automatic update capability.</p> <p><u>DFAS-Cleveland</u> All workstations and servers at DFAS-Cleveland use antivirus software, which has an automatic update capability.</p> <p><u>DFAS-Indianapolis</u> All workstations and servers at DFAS-Indianapolis use antivirus software, which has an automatic update capability.</p>	<p><u>DFAS-Arlington</u> Observed that servers, workstations, and mobile computing devices implemented virus protection that included a capability for automatic updates for all DDRS locations.</p> <p>Inspected a screen print as evidence that these settings had been configured.</p> <p><u>DFAS-Cleveland</u> Observed that servers, workstations, and mobile computing devices implemented virus protection that included a capability for automatic updates for all DDRS locations.</p> <p>Inspected a screen print as evidence that these settings had been configured.</p> <p><u>DFAS-Indianapolis</u> Observed that servers, workstations, and mobile computing devices implemented virus protection that included a capability for automatic updates for all DDRS locations.</p> <p>Inspected a screen print as evidence that these settings had been configured.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p> <p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
39	All VPN traffic is visible to network Intrusion Detection System (IDS).	<u>DISA DECC-Ogden</u> All external Virtual Private Network traffic coming into DISA DECC-Ogden is visible to the IDS.	<u>DISA DECC-Ogden</u> Inquired of the System Administrators to confirm that all VPN traffic was visible to the network IDS.	<u>DISA DECC-Ogden</u> No relevant exceptions noted.
40	At a minimum, robust Commercial off-the-shelf Information Assurance enabled products are used to protect sensitive information when the information uses public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system.	<u>DISA DECC-Ogden</u> No public network is used. The DoD Non-secure Internet Protocol Router Network is used. <u>DFAS-Arlington</u> All DDRS application data is communicated between the user and the production server using encryption transfer protocol capability. DDRS information does not use public networks.	<u>DISA DECC-Ogden</u> Performed network monitoring using the Securify tool to test for unencrypted traffic transmitted over commercial or wireless networks. <u>DFAS-Arlington</u> Performed network monitoring using the Securify tool to verify that Hyper Text Transfer Protocol Secure traffic was used to communicate between the end-users and the server.	<u>DISA DECC-Ogden</u> No relevant exceptions noted. <u>DFAS-Arlington</u> No relevant exceptions noted.
41	Unless there is an overriding technical or operational problem, workstation screen-lock-out function is associated with each workstation.	<u>DISA DECC-Ogden</u> All workstations automatically lock out after 15 minutes of inactivity. Also all work stations can be manually locked by the user at anytime. <u>DFAS-Arlington</u> At DFAS-Arlington, the workstation screen-lock functionality is associated with each workstation. Users can invoke this screen lock-out function by removing their Common Access Card (CAC) card from the reader or by	<u>DISA DECC-Ogden</u> Confirmed through observation that the workstation screen lock-out function was applied. If they were not being used, inquired of the System Administrator to determine why the screen lock-out function was not being used. <u>DFAS-Arlington</u> Confirmed through observation that the workstation screen lock-out function was applied.	<u>DISA DECC-Ogden</u> No relevant exceptions noted. <u>DFAS-Arlington</u> No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>entering Ctrl-Alt-Delete followed by the enter key.</p> <p><u>DFAS-Cleveland</u> At DFAS-Cleveland, workstation screen lock-out function is associated with each workstation. Users can invoke the screen lock-out function by removing their CAC card from the reader or by entering Ctrl-Alt-Delete followed by the enter key.</p> <p><u>DFAS-Indianapolis</u> At DFAS-Indianapolis the workstation screen lock-out function is available with each workstation. Users can invoke this function by removing their CAC card from the reader or by entering Ctrl-Alt-Delete followed by the enter key.</p>	<p><u>DFAS-Cleveland</u> Confirmed through observation that workstation screen-lock-out function was applied.</p> <p><u>DFAS-Indianapolis</u> Confirmed through observation that the workstation screen lock-out function was applied.</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>
42	Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within DoD information systems.	<p><u>DISA DECC-Ogden</u> Instant messaging traffic is not allowed per DoD Policy.</p> <p><u>DFAS-Arlington</u> Instant messaging users at DFAS-Arlington are restricted to DoD instant messaging servers.</p> <p><u>DFAS-Cleveland.</u> Instant messaging traffic is not allowed per DoD Policy.</p>	<p><u>DISA DECC-Ogden</u> Performed network monitoring using the Securify tool to test for instant messaging traffic to the DDRS servers.</p> <p><u>DFAS-Arlington</u> Performed network monitoring using the Securify tool to test for instant messaging traffic to the DDRS servers.</p> <p><u>DFAS-Cleveland</u> Performed network monitoring using the Securify tool to test for instant messaging traffic to the DDRS servers.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p> <p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<u>DFAS-Indianapolis</u> Instant messaging traffic is not allowed per DoD Policy.	<u>DFAS-Indianapolis</u> Performed network monitoring using the Securify tool to test for instant messaging traffic to the DDRS servers.	<u>DFAS-Indianapolis</u> No relevant exceptions noted.
43	For Automated Information System applications, a list of all (potential) hosting enclaves is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements.	<u>DISA DECC-Ogden</u> DISA DECC-Ogden requires a Service Level Agreement (SLA) with every customer and a copy of the system's SSAA. The SLA and the SSAA contain the requirements for system and data criticality, maximum acceptable downtime, and any additional continuity of operations support that may be required. Standard DISA procedures provide for the daily backup of critical data and the offsite storage of such data as required allowing for the resumption of normal processing in the event of scheduled or unscheduled system interruptions or downtime. Each SLA provides the particulars for that organization's system requirements, to include the backup and recovery process and procedures to be followed as well as the maximum downtime that is considered acceptable.	<u>DISA DECC-Ogden</u> Read the DISA DECC-Ogden SLA to confirm the DDRS hosting enclave had been identified and documented. Performed network monitoring testing using the Securify tool to determine whether the DDRS Internet Protocol address was within the DISA DECC-Ogden hosting enclave.	<u>DISA DECC-Ogden</u> No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
44	Group authenticators for application or network access may be used only in conjunction with an individual authenticator.	<p><u>DISA DECC-Ogden</u> Root is a shared account among the DDRS system administrators. Individual authenticators are required to access the DDRS Operating System.</p> <p><u>DFAS-Indianapolis</u> The DDRS DBA support team members in Indianapolis each have their own Unix account for each platform in Ogden that supports the DDRS application. DBAs share the Oracle UNIX account but they cannot login to that account directly. DBAs must login to the platform with their unique account and then Su (Switch User) to the Oracle account.</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of the DDRS System Administrator the process for obtaining an administrator account on the DDRS Operating System.</p> <p>Inspected all nine SAAR forms to confirm that a form was on file for all System Administrators with access to the DDRS Operating System.</p> <p><u>DFAS-Indianapolis</u> Inquired of the DDRS Project Manager and the lead DBA of the process for granting the DBA access to DDRS.</p> <p>Inspected all six SAAR forms to confirm that a form was on file for DBAs with access to DDRS.</p> <p>Inquired of the end user account administrator regarding DDRS end user account creation, modification, deletion, and password reset process for DDRS.</p>	<p><u>DISA DECC-Ogden</u> Seven of nine SAAR forms inspected did not have the signature of the Information Assurance Officer on the SAAR form.</p> <p>One System Administrator did not have a SAAR form on file. Additionally, access had not been removed for that user in a timely manner. This user's access was subsequently deleted because he no longer required access to DDRS.</p> <p><u>DFAS-Indianapolis</u> One of six SAAR forms for DBAs did not have the justification for access completed on the SAAR form.</p> <p>None of the six SAAR forms inspected for DBAs had the signatures of the Functional Data Owner and Information Assurance Officer.</p> <p>One of six DBAs approved his own SAAR form.</p>
45	To help prevent inadvertent disclosure of controlled information, all contractors and foreign nationals are identified by e-mail addresses and display names.	<p><u>DISA DECC-Ogden</u> All DISA DECC-Ogden e-mails addresses are compliant with the control objective. DISA DECC-Ogden does not control other e-mail addresses within</p>	<p><u>DISA DECC-Ogden</u> Inspected the e-mail addresses of all DDRS-related personnel at DISA DECC-Ogden to confirm that contractors and foreign</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>DDRS or Tech POC e-mail address lists.</p> <p>To prevent inadvertent disclosure of controlled information, all contractors are identified by the abbreviation "ctr" and all foreign nationals are identified by their two-character country code.</p> <p><u>DFAS-Arlington</u> Contractors at DFAS-Arlington are identified as such in their e-mail display name.</p> <p><u>DFAS-Cleveland</u> Contractors at DFAS-Cleveland are identified as such in their e-mail display name.</p> <p><u>DFAS-Indianapolis</u> Contractors at DFAS-Indianapolis are identified as such in their e-mail display name.</p>	<p>nationals were identified in their e-mail addresses and display names.</p> <p><u>DFAS-Arlington</u> Inspected the e-mail addresses of all DDRS-related individuals at DFAS-Arlington to confirm that contractors and foreign nationals were identified in their e-mail addresses and display names.</p> <p><u>DFAS-Cleveland</u> Inspected the e-mail addresses of all DDRS-related individuals at DFAS-Cleveland to confirm that contractors and foreign nationals were identified in their e-mail addresses and display names.</p> <p><u>DFAS-Indianapolis</u> Inspected the e-mail addresses of all DDRS-related individuals at DFAS-Indianapolis to confirm that contractors and foreign nationals were identified in their e-mail addresses and display names.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p> <p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
46	Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using National Institute of Standards and Technology certified cryptography.	<u>DISA DECC-Ogden</u> DDRS does not use a commercial or wireless network to transmit data. All data coming into DDRS from outside DISA DECC-Ogden is through File Transfer Protocol (FTP) or VPN communications.	<u>DISA DECC-Ogden</u> Performed network monitoring using the Securify tool to verify that Hyper Text Transfer Protocol Secure traffic was used to communicate between the end-users and server. Performed network monitoring using the Securify tool to test for unencrypted traffic transmitted over commercial or wireless networks.	<u>DISA DECC-Ogden</u> No relevant issues noted.
47	Discretionary access controls are a sufficient Information Assurance mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rules.	<u>DFAS-Arlington</u> There are no system interfaces with DDRS.	<u>DFAS-Arlington</u> Inquired of the Information Assurance Officer to confirm there were no automated system interfaces for DDRS. Read the DDRS SSAA to confirm that data had been assigned a classification level and that there were no automated system interfaces.	<u>DFAS-Arlington</u> There were no automated system interfaces identified. No relevant exceptions noted.
48	Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures is planned, scheduled, and conducted.	<u>DISA DECC-Ogden</u> DISA DECC-Ogden performs a monthly Information Security System scan. The monthly Information Security System scan is not announced. Automated SRR scripts are run on each server and reported to the Montgomery SRR database on a weekly basis.	<u>DISA DECC-Ogden</u> Confirmed through inquiry that conformance testing was performed. That it included periodic, unannounced, in-depth monitoring, and provided for specific penetration testing to confirm compliance with all vulnerability mitigation procedures was planned, scheduled, and conducted.	<u>DISA DECC-Ogden</u> No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>Inspected Information System Security scans and inspected evidence that conformance and penetration testing was being completed.</p> <p>Inspected physical penetration testing documentation for DISA DECC-Ogden.</p>	
49	All users are warned that they are entering a Government information system.	<p><u>DISA DECC-Ogden</u> All users are warned that they are entering a Government information system before gaining access to the network or system. All users must view a warning banner on each access to DDRS.</p> <p><u>DFAS-Arlington</u> All users are warned that they are entering a Government information system before gaining access to the network or system. All users must view a warning banner on each access to DDRS.</p> <p><u>DFAS-Cleveland</u> All users are warned that they are entering a Government information system before gaining access to the network or system. All users must view a warning banner on each access to DDRS.</p> <p><u>DFAS-Indianapolis</u> All users are warned that they are entering a Government information system before gaining access to the</p>	<p><u>DISA DECC-Ogden</u> Observed that a sample of workstations displayed a DoD warning banner.</p> <p><u>DFAS-Arlington</u> Observed that a sample of workstations displayed a DoD warning banner.</p> <p><u>DFAS-Cleveland</u> Observed that a sample of workstations displayed a DoD warning banner.</p> <p><u>DFAS-Indianapolis</u> Observed that a sample of workstations displayed a DoD warning banner.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p> <p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		network or system. All users must view a warning banner on each access to DDRS.		
50	Information and DoD information systems that store, process, transmit, or display data in any form or format that is not approved for public release comply with all requirements in policy and guidance documents.	<p><u>DISA DECC-Ogden</u> The DECC-Ogden environment and network operates under the security provisions of public law, Executive Orders, Department of Defense directives and regulations, and DISA instructions, guides, and handbooks.</p> <p><u>DFAS-Arlington</u> DDRS prepares and displays financial reports in compliance with the DoD Financial Management Regulation (http://www.dod.mil/comptroller/fmr/). Reports containing user names are labeled in accordance with DoD 5200.1-</p>	<p><u>DISA DECC-Ogden</u> Confirmed through observation that workstation screen-lock functionality was applied. If screen lock-outs were not being used, we met with a System Administrator to confirm the reason.</p> <p>Inquired key personnel to confirm that information in transit through a network at the same classification level was encrypted.</p> <p>Performed network monitoring to confirm traffic transmitted over commercial networks was encrypted.</p> <p>Observed that displays and printers used for sensitive but unclassified information were positioned to deter unauthorized individuals from reading the information at all the locations.</p> <p><u>DFAS-Arlington</u> Confirmed through observation that workstation screen lock-out function was applied.</p> <p>Observed that displays used for DDRS activities were positioned</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		R, Appendix 3.	to deter unauthorized individuals from reading the information.	
51	Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with National Institute of Standards and Technology certified cryptography.	<u>DISA DECC-Ogden</u> Information is encrypted with National Institute of Standards and Technology certified cryptography.	<u>DISA DECC-Ogden</u> Performed network monitoring using the Securify tool to confirm information was encrypted.	<u>DISA DECC-Ogden</u> No relevant exceptions noted.
52	Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a Demilitarized Zone (DMZ).	<u>DISA DECC-Ogden</u> Systems that require public access are placed in an isolated subnet in a DMZ for the security of those systems without impacting the remainder of the subnets within the environment. The DDRS DMZ is located at DISA DECC-Ogden.	<u>DISA DECC-Ogden</u> Inspected the DISA DECC-Ogden system architecture to confirm that connections between DoD enclaves and the Internet were configured with a DMZ.	<u>DISA DECC-Ogden</u> No relevant exceptions noted.
53	Boundary defense mechanisms to include firewalls and network IDS are deployed at the enclave boundary.	<u>DISA DECC-Ogden</u> DISA DECC-Ogden has four Class C networks that are used for different purposes as well as one Class B network. The premise routers are configured to only let authenticated networks with a justified requirement through to systems on the DISA DECC-Ogden networks. All production systems are protected by two Juniper M20 premise routers. Additionally, an Intrusion Detection System has been implemented for DISA DECC-Ogden.	<u>DISA DECC-Ogden</u> Inspected the DISA DECC-Ogden system architecture to confirm that boundary defense mechanisms to include firewalls and network Intrusion Detection Systems were deployed at the enclave boundary. Inspected a system network diagram and read the diagram with the System Administrator to confirm that defense mechanisms were employed. Observed the existence of firewalls and Intrusion Detection Systems.	<u>DISA DECC-Ogden</u> No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
54	<p>Devices that display or output classified or sensitive but unclassified information in human readable form are positioned to deter unauthorized individuals from reading the information.</p>	<p><u>DISA DECC-Ogden</u> The DDRS system administrators are located in cubicles and their monitors are placed so that only personnel inside the cubicle could view the information the monitor displayed.</p> <p><u>DFAS-Arlington</u> DFAS-Arlington printers and displays are controlled within a secured building. The DDRS PMO staff is located in cubicles and their monitors are placed so that only individuals inside the cubicle can view the information the monitor displays.</p> <p><u>DFAS-Cleveland</u> The DDRS development staff is located in cubicles and their monitors are placed so that only individuals inside the cubicle could view the information the monitor displays.</p> <p><u>DFAS-Indianapolis</u> The DDRS DBA staff is located in cubicles and their monitors are placed so that only individuals inside the cubicle view the information it displays.</p>	<p><u>DISA DECC-Ogden</u> Observed that displays used for DDRS activities were positioned to deter unauthorized individuals from reading the information.</p> <p><u>DFAS-Arlington</u> Observed that displays used for DDRS activities were positioned to deter unauthorized individuals from reading the information.</p> <p><u>DFAS-Cleveland</u> Observed that displays used for DDRS activities were positioned to deter unauthorized individuals from reading the information.</p> <p><u>DFAS-Indianapolis</u> Observed that displays used for DDRS activities were positioned to deter unauthorized individuals from reading the information.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p> <p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>
55	<p>Individuals requiring access to sensitive information are processed for access authorization in accordance with DoD personnel security policies.</p>	<p><u>DISA DECC-Ogden</u> The SAAR form is sent to DISA DECC-Ogden, which verifies required field contents and signatures and creates user IDs and passwords and files the SAAR form. All DISA civilians are required to have a minimum of a Secret Clearance or interim Secret Clearance prior to</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of the Security Assurance Manager the process of recording security clearances for DISA DECC-Ogden staff.</p> <p>Confirmed that background investigations had been</p>	<p><u>DISA DECC-Ogden</u> Seven of nine SAAR forms inspected did not have the signature of the Information Assurance Officer on the SAAR form.</p> <p>One System Administrator did not have a SAAR form on file.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>physical or system access being granted. New contractors are submitted for investigation and Interim Information Technology access granted by DISA Personnel Security or an Interim clearance from Defense Investigative Security Clearance Office is obtained prior to physical or system access being granted.</p> <p><u>DFAS-Arlington</u> All individuals requiring access to DDRS must have their Security Manager's approval on the SAAR form before access is granted. The Information Assurance Officer or Assistant Information Assurance Officer verifies the field contents and signatures before creating or requesting the creation of each user ID and password.</p> <p><u>DFAS-Cleveland</u> All individuals requiring access to DDRS must have their Security Manager's approval on the SAAR form</p>	<p>performed and were recurring on an appropriate schedule for individuals with access to the DDRS Operating System.</p> <p>Confirmed through inquiry of the DDRS System Administrator the process for obtaining an administrator account on the DDRS Operating System.</p> <p>Inspected all nine SAAR forms to confirm that a form was on file for all System Administrators with access to the DDRS Operating System.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry of the Personnel Security Program Manager of the process of recording security clearances for DFAS personnel.</p> <p>Inspected all 18 SAAR forms to confirm that a form was on file for the DDRS PMO staff with access to DDRS.</p> <p>Inspected all 22 access forms to confirm that a form was on file for PMO staff with access to the CMIS.</p> <p><u>DFAS-Cleveland</u> Confirmed through inquiry of the DDRS Configuration Manager, PVCS Configuration</p>	<p>Additionally, access had not been removed for that user in a timely manner. This user's access was subsequently deleted because he no longer required access to DDRS.</p> <p><u>DFAS-Arlington</u> Three of 18 SAAR forms did not document justification for access completed; another three of 18 did not document type of system access.</p> <p>One of 22 CMIS PMO users had access to roles that were not required for his duties.</p> <p>Seven of 22 CMIS PMO users were former DDRS PMO staff, but their access to CMIS had not been terminated.</p> <p><u>DFAS-Cleveland</u> There were no forms used to track PVCS access.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>before access is granted. The Information Assurance Officer or Assistant Information Assurance Officer verifies the field contents and signatures before creating or requesting the creation of each user ID and password.</p> <p><u>DFAS-Indianapolis</u> The DDRS DBA staff is required to complete a SAAR form to obtain a user ID. This form includes a section that must be completed by the security office verifying the employee clearance level. Until security clearance is verified and the SAAR form is signed, the user cannot log in to any system. The processing of the SAAR form and its status are tracked by the individual team leads until completion.</p>	<p>Manager, and DDRS Budgetary Module Team Lead the process for recording access to the CMIS, the PVCS, and the Oracle Versioning application.</p> <p>Inspected CMIS access forms to confirm that a form was on file for the 33 DDRS development staff with access to the CMIS.</p> <p>Inspected all 31 6i Repository User Access Forms for DFAS-Cleveland DDRS staff members to confirm that a form was on file for the DDRS development staff with access to the Oracle Versioning System.</p> <p>Requested access forms to confirm that a form was on file for DDRS development staff with access to the PVCS.</p> <p><u>DFAS-Indianapolis</u> Verified that background investigations had been performed and were reoccurring on an appropriate schedule for individuals with access to the DDRS database.</p> <p>Inspected all six SAAR forms to confirm that a form was on file for the DBAs with access to DDRS.</p>	<p><u>DFAS-Indianapolis</u> One of six SAAR forms for DBAs did not have the justification for access completed on the SAAR form.</p> <p>None of the six SAAR forms inspected for DBAs had the signatures of the Functional Data Owner and Information Assurance Officer.</p> <p>One of six DBAs approved his own SAAR form.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
56	DoD information systems comply with DoD ports, protocols, and services guidance.	<u>DISA DECC-Ogden</u> DDRS ports, protocols, and services are in accordance with the DISA STIGs.	<u>DISA DECC-Ogden</u> Confirmed through the performance of network monitoring using the Securify tool that DDRS complied with DoD ports, protocols, and services guidance.	<u>DISA DECC-Ogden</u> The test results have been removed from the SAS 70 Report due to the sensitivity of the information contained in the test results.
57	Binary or machine executable public domain software products and other software products with limited or no warranty are not used in DoD information systems.	<u>DISA DECC-Ogden</u> Open source programs are allowed after going through a test and review process defined by the DISA Field Service Office.	<u>DISA DECC-Ogden</u> Read inventory listing to confirm that binary or machine executable public domain software products and other software products with limited or no warranty were not installed on DDRS.	<u>DISA DECC-Ogden</u> The test results have been removed from the SAS 70 Report due to the sensitivity of the information contained in the test results.
<i>Application Software Development and Change Control</i>				
58	A system development life cycle methodology has been implemented and documented.	<u>DFAS-Cleveland</u> The DDRS Software Quality Assurance Plan identifies a life cycle methodology, which incorporates Software Quality Assurance Plan milestones, configuration management, and other management events including the domain of DDRS Policy applicability. <u>DFAS-Indianapolis</u> A DoD specific system development life cycle is operational and utilized for the development of the application software.	<u>DFAS-Cleveland</u> Read the Software Quality Assurance Plan to confirm that it existed and was current. <u>DFAS-Indianapolis</u> Read the International Organizational for Standardization Mid-Tier Guidelines and Procedures to confirm that it existed and was current. Read the DFAS Corporate Information Infrastructure Common Elements Release	<u>DFAS-Cleveland</u> No relevant exceptions noted. <u>DFAS-Indianapolis</u> No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			Management DDRS step-by-step MOD Creation Procedure to confirm that it existed and was current.	
59	Authorizations for software modifications are documented and maintained.	<p><u>DFAS-Cleveland</u> A DDRS Configuration Management Plan is observant of authorized modifications, additions, and deletions, which are documented and maintained in the interest of process and product integrity.</p> <p><u>DFAS-Indianapolis</u> A configuration management group and a release management group are responsible for maintaining the changes</p>	<p><u>DFAS-Cleveland</u> Inspected all six DDRS-AFS releases, which occurred during the seven month period under review from October 2004 to April 2005, and obtained the artifact documentation to confirm the Functional Requirements Review, Change Control Board, Critical Design Review, Test Readiness Review and Systems Integration Testing , Test Readiness Review, Functional Validation Testing, Test Readiness Review and Concurrent Validation Testing, Release Implementation Readiness Review, and Post Implementation Review contained appropriate signatures for authorizing the modification to DDRS.</p> <p>Inquired of DFAS-Cleveland personnel to corroborate the results of the testing.</p> <p><u>DFAS-Indianapolis</u> Inquired of DFAS-Indianapolis personnel about the process for documenting and maintaining</p>	<p><u>DFAS-Cleveland</u> The following exceptions were noted:</p> <ul style="list-style-type: none"> • Two of six changes lacked a Functional Requirements Review Statement of Agreement; • One of six changes did not have a Test Readiness Review and Systems Integration Testing Statement of Agreement; • One of six changes did not have a Test Readiness Review and Functional Validation Testing Statement of Agreement; • Two of six changes did not have a Release Implementation Readiness Review Statement of Agreement; and, • One of six changes did not have a Post Implementation Review signature. <p><u>DFAS-Indianapolis</u> We were unable to trace software modifications from DFAS-Cleveland to the changes</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		requested via a formal system change request and each release is a documented process.	authorizations for software modifications.	implemented by DFAS-Indianapolis on the production servers because the DFAS-Indianapolis DBAs were unable to determine how to match the modifications to the system change request maintained by DFAS-Cleveland.
60	Use of public domain and personal software is restricted.	<u>DISA DECC-Ogden</u> Open source programs are allowed after going through a test and review process defined by the DISA Field Service Office.	<u>DISA DECC-Ogden</u> Read inventory listing to confirm that binary or machine executable public domain software products and other software products with limited or no warranty were not installed on DDRS.	<u>DISA DECC-Ogden</u> The test results have been removed the SAS 70 Report due to the sensitivity of the information contained in the test results.
61	Changes are controlled as programs progress through testing to final approval.	<u>DFAS-Cleveland</u> A DDRS Configuration Management Plan is observant of authorized modifications, additions, and deletions which are documented and maintained in the interest of process and product integrity.	<u>DFAS-Cleveland</u> Inspected all six changes to confirm that the artifact documentation Functional Requirements Review, Change Control Board, Critical Design Review, Test Readiness Review and Systems Integration Testing, Test Readiness Review, Functional Validation Testing, Test Readiness Review and Concurrent Validation Testing, Release Implementation Readiness Review, and Post Implementation Review was available, complete and authorized for modifications to DDRS.	<u>DFAS-Cleveland</u> The following exceptions were noted during our testing of all six DDRS-AFS module releases. We noted the following missing elements: Function Requirements Review Statement of Agreement; Test Readiness Review and Systems Integration Testing Checklist; Test Readiness Review and Systems Integration Testing Attendee List; Test Readiness Review and Systems Integration Testing Open Item List; Test Readiness Review and Systems Integration Testing Statement of Agreement; Test Readiness Review and Functional Validation Testing Checklist; Test Readiness Review and Functional Validation

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Indianapolis</u> DDRS employs the CMIS and Oracle's Designer Repository to control programs and their progress throughout testing and final approval. The Release Management Group also controls changes to the production environment and maintains an audit trail on application changes.</p>	<p>Inquired of DFAS-Cleveland personnel to corroborate the results of the testing. Read the SPI policies and confirmed they described the process that changes must go through to be implemented.</p> <p><u>DFAS-Indianapolis</u> Inquired of DFAS-Indianapolis personnel about the process for controlling changes for software modifications.</p>	<p>Testing attendee list; Test Readiness Review and Functional Validation Testing open item list; Test Readiness Review and Functional Validation Testing, Statement of Agreement; Functional Validation Testing Certification Form; Release Implementation Readiness Review Statement of Agreement; Post Implementation Readiness Review Signature; Final Physical Configuration Audit; and Final Functional Configuration Audit.</p> <p><u>DFAS-Indianapolis</u> We were unable to trace software modifications from DFAS-Cleveland to the changes implemented by DFAS-Indianapolis on the DDRS production servers because the DFAS-Indianapolis DBAs were unable to determine how to match the modifications to the system change requests maintained by DFAS-Cleveland.</p>
62	Emergency changes are promptly randomly sampled and approved before being moved into production.	<p><u>DFAS-Cleveland</u> Emergency changes are handled by creating an Emergency Release Waiver. Changes are required to be randomly sampled before being moved into production.</p>	<p><u>DFAS-Cleveland</u> Inspected a random sample of changes to confirm that an Emergency Release Waiver was created, completed and authorized by appropriate personnel when necessary. Inquired of DFAS-Cleveland personnel to corroborate the results of the testing.</p>	<p><u>DFAS-Cleveland</u> No relevant exception noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Indianapolis</u> Emergency changes are handled in the same manner as the normal release processes. A configuration management group and a release management group are responsible for maintaining the changes requested via a formal system change request and each release is a documented process.</p>	<p><u>DFAS-Indianapolis</u> Inquired of DFAS-Indianapolis personnel on the process of documenting and maintaining authorizations for emergency software modifications.</p>	<p><u>DFAS-Indianapolis</u> We were unable to trace software modifications from DFAS-Cleveland to the changes implemented by DFAS-Indianapolis on the DDRS production servers because the DFAS-Indianapolis DBAs were unable to determine how to match the modifications to the system change requests maintained by DFAS-Cleveland.</p>
63	Distribution and implementation of new or revised software is controlled.	<p><u>DFAS-Indianapolis</u> The Technology Services Organization and Corporate Services control the submission of software or application changes into the production environment. The DDRS developers submit changes via File Transfer Protocol to an inbox on a Technology Services Organization platform. The announcement is made via e-mail to Technology Services Organization release management. Release Management picks up the submittal and relays the changes to the DBA staff using File Transfer Protocol. These changes are then used on the appropriate DISA server or platform.</p>	<p><u>DFAS-Indianapolis</u> Inquired of DFAS-Indianapolis personnel about the process for distributing and releasing software modifications.</p>	<p><u>DFAS-Indianapolis</u> We were unable to trace software modifications from DFAS-Cleveland to the changes implemented by DFAS-Indianapolis on the DDRS production servers because the DFAS-Indianapolis DBAs were unable to determine how to match the modifications to the system change requests maintained by DFAS-Cleveland.</p>
64	Programs are labeled and inventoried.	<p><u>DFAS-Cleveland</u> The DFAS Corporate Information Infrastructure Naming Standard document is utilized for labeling and inventorying programs.</p>	<p><u>DFAS-Cleveland</u> Inspected a random sample of 930 configuration items to determine compliance with naming standards and to confirm they were inventoried.</p>	<p><u>DFAS-Cleveland</u> The DFAS Corporate Information Infrastructure naming standards were not followed for DDRS items.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
65	Access to program libraries is restricted to appropriate personnel.	<p><u>DFAS-Cleveland</u> DFAS-Cleveland grants role based access to each member of the DDRS development team on joining the team, and periodically when Corporate Services requires it.</p> <p><u>DFAS-Indianapolis</u> Access to development tools such as CMIS, PVCS and Oracle Versioning is controlled through standard procedures and documented request forms.</p>	<p><u>DFAS-Cleveland</u> Confirmed the process for recording access to the CMIS, the PVCS, and the Oracle Versioning application through inquiry of the following DDRS personnel: DDRS Configuration Manager; PVCS; Configuration Manager; and DDRS Budgetary Module Team Lead.</p> <p>Inspected CMIS access forms to confirm that a form was on file for the 33 DDRS development staff with access to the CMIS. Inspected all 6i Repository User Access Forms for a sample of 31 DFAS-Cleveland DDRS staff members to confirm that a form was on file for the DDRS development staff with access to the Oracle Versioning System.</p> <p>Requested access forms to confirm that a form was on file for DDRS development staff with access to the PVCS.</p> <p><u>DFAS-Indianapolis</u> Inquired of the DDRS Project Manager and the lead DBA of the process for granting the DBA access to DDRS.</p> <p>Inspected all six SAAR forms to confirm that a form was on file for the DDRS DBAs with access to DDRS.</p>	<p><u>DFAS-Cleveland</u> There were no forms used to track access to the PVCS.</p> <p><u>DFAS-Indianapolis</u> One of six SAAR forms for DBAs did not have the justification for access completed on the SAAR form.</p> <p>None of the six SAAR forms inspected for DBAs had the signatures of the Functional Data Owner and Information Assurance</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				<p>Officer.</p> <p>One of six DBAs approved his own SAAR form.</p> <p>DFAS-Indianapolis DBAs had full access to the DDRS test, development, and production environments.</p>
66	<p>Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities.</p>	<p><u>DFAS-Indianapolis</u> The Statement of Work governs the explicit roles and responsibilities for any service provider that bids on services for the DDRS system.</p> <p><u>DFAS-Arlington</u> The DDRS PMO outsources the Central Design Agency, Database Administrator, and application hosting Information Technology services to DFAS-Cleveland, DFAS-Indianapolis, and DISA DECC-Ogden, respectively. Each agreement delineates roles and responsibilities.</p>	<p><u>DFAS-Indianapolis</u> Inspected the Statement of Work contract agreement to confirm that it expressly addressed Government, service provider, and end-user IA roles and responsibilities.</p> <p><u>DFAS-Arlington</u> Inspected the SOW contract agreement to confirm that it expressly addressed Government, service provider, and end-user IA roles and responsibilities.</p> <p>Inquired of DFAS-Arlington personnel to corroborate the results of the testing.</p>	<p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
67	The acquisition of all Information Assurance- and Information Assurance-enabled Government Off-the-Shelf Information Technology products is limited to products that have been evaluated by the National Security Agency or in accordance with National Security Agency approved processes.	<u>DFAS-Arlington</u> All Government off-the-shelf Information Technology products used in DDRS have been evaluated by the common criteria or are under evaluation.	<u>DFAS-Arlington</u> Confirmed through inquiry that DDRS was not a Government Off-the-Shelf product.	<u>DFAS-Arlington</u> No relevant exceptions noted.
68	Movement of programs and data among libraries is controlled.	<u>DFAS-Cleveland</u> The development team conducts Test Readiness Reviews-System Integration Testing, Test Readiness Reviews-Functional Validation Testing, and Release Implementation Readiness Review, and produces or defines ARCs compression format at the time of implementation readiness. Changes are released to the Release Management Group at DFAS-Indianapolis for implementation.	<u>DFAS-Cleveland</u> Inspected a sample of six changes to confirm that the artifact testing documentation Test Readiness Review and System Integration Testing, Test Readiness Review and Functional Validation Testing, Test Readiness Review and Change Validation Testing, and Release Implementation Readiness Review was available, complete, and authorized for modifications to DDRS. Inquired of DFAS-Cleveland personnel to corroborate the results of the testing.	<u>DFAS-Cleveland</u> The following exceptions were noted during our testing of all six DDRS-AFS module releases. We noted the following missing elements: Function Requirements Review Statement of Agreement; Test Readiness Review and Systems Integration Testing Checklist; Test Readiness Review and Systems Integration Testing Attendee List; Test Readiness Review and Systems Integration Testing Open Item List; Test Readiness Review and Systems Integration Testing Statement of Agreement; Test Readiness Review and Functional Validation Testing Checklist; Test Readiness Review and Functional Validation Testing attendee list; Test Readiness Review and Functional Validation Testing open item list; Test Readiness Review and Functional Validation Testing, Statement of Agreement; Functional Validation Testing Certification Form; Release

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Indianapolis</u> DDRS employs CMIS to control the movement of information programs and data among libraries. The process includes sign off by responsible individuals authorizing the actions.</p>	<p><u>DFAS-Indianapolis</u> Inquired of personnel at DFAS-Indianapolis about the process for controlling movement of programs and data among libraries.</p>	<p>Implementation Readiness Review Statement of Agreement; Post Implementation Readiness Review Signature; Final Physical Configuration Audit; and Final Functional Configuration Audit.</p> <p><u>DFAS-Indianapolis</u> We were unable to trace software modifications from DFAS-Cleveland to the changes implemented by DFAS-Indianapolis on the DDRS production servers because DFAS-Indianapolis DBAs were unable to determine how to match the modifications to the System Change Requests maintained by DFAS-Cleveland.</p>
69	<p>Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability such as buffer over runs such as are specified for all software development initiatives.</p>	<p><u>DFAS-Cleveland</u> A Software Quality Assurance Program has been instituted for all DDRS projects. This program is executed during the lifecycle of all DDRS releases in accordance with DFAS Policy SM-13. A key element of the software quality assurance function is to help to develop and observe the adherence to DDRS policies.</p>	<p><u>DFAS-Cleveland</u> Inspected all six changes to verify that a software quality assurance member was present at each meeting through review of attendee listings.</p> <p>Inspected all six changes to confirm that the artifact testing documentation (Test Readiness Review and Systems Integration Testing, Test Readiness Review and Functional Validation Testing, and Test Readiness Review and Change Validation Testing) was available, complete and authorized for modifications to DDRS.</p>	<p><u>DFAS-Cleveland</u> The following exceptions were noted during our testing of all six DDRS-AFS module releases. We noted the following missing elements: FRR SQA Presence; Function Requirements Review Statement of Agreement; Test Readiness Review and Systems Integration Testing Checklist; Test Readiness Review and Systems Integration Testing Attendee List; Test Readiness Review and Systems Integration Testing Open Item List; Test Readiness Review and Systems Integration Testing Statement of Agreement; Test Readiness Review and Functional</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			Inquired of key DFAS-Cleveland personnel to corroborate the results of the testing above.	Validation Testing Checklist; Test Readiness Review and Functional Validation Testing attendee list; Test Readiness Review and Functional Validation Testing open item list; Test Readiness Review and Functional Validation Testing, Statement of Agreement; Functional Validation Testing Certification Form; Release Implementation Readiness Review Statement of Agreement; Post Implementation Readiness Review Signature; Final Physical Configuration Audit; and Final Functional Configuration Audit.
	<i>System Software Controls</i>			
70	Access authorizations are appropriately limited.	<u>DISA DECC-Ogden</u> Access to system software is restricted to personnel with corresponding job responsibilities by access control software. Update access should generally be limited to primary and backup systems programmers.	<u>DISA DECC-Ogden</u> Read the policies and procedures for restricting access to the systems software to confirm that they were current. Inspected all nine SAAR forms to confirm that a form was on file for all System Administrators with access to the DDRS Operating System.	<u>DISA DECC-Ogden</u> Seven of nine SAAR forms inspected did not have the signature of the Information Assurance Officer on the SAAR form. One System Administrator did not have a SAAR form on file. Additionally, access had not been removed for that user in a timely manner. This user's access was subsequently deleted because he no longer required access to DDRS.
71	All access paths have been identified and controls implemented to prevent or detect access for all paths.	<u>DISA DECC-Ogden</u> Auditing is enabled on all DDRS servers at the Operating System level. The UNIX STIG is enforced on all DDRS servers.	<u>DISA DECC-Ogden</u> Confirmed through inquiry of an IT Specialist that audit trails were created and reviewed for the DDRS Operating System.	<u>DISA DECC-Ogden</u> DISA DECC-Ogden did not proactively monitor or review audit trails.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>The Operating System is configured to prevent circumvention of the security software and application controls. Access to system software is restricted to personnel with corresponding job responsibilities by access control software. Update access should generally be limited to primary and backup systems programmers.</p>	<p>Confirmed through inquiry of the Lead Firewall Technician and Communications Chief and observation that all access paths were monitored.</p>	
72	<p>Policies and techniques have been implemented for using and monitoring the use of system utilities.</p>	<p><u>DISA DECC-Ogden</u> Audit logs are used to monitor the use of system utilities.</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of an IT Specialist that audit trails were created and reviewed for the DDRS Operating System.</p> <p>Read a sample of the audit logs from the DDRS servers to confirm that Ogden personnel reviewed the logs on a regular basis and that any issues noted were documented and researched.</p> <p>Inspected all nine SAAR forms to confirm that a form was on file for all System Administrators with access to the DDRS Operating System.</p> <p>Confirmed through inquiry of the System Administrators that the super user log was created and reviewed.</p>	<p><u>DISA DECC-Ogden</u> DISA DECC-Ogden did not proactively monitor or review audit trails.</p> <p>Seven of nine SAAR forms inspected did not have the signature of the Information Assurance Officer on the SAAR form.</p> <p>One System Administrator did not have a SAAR form on file. Additionally, access had not been removed for that user in a timely manner. This user's access was subsequently deleted because he no longer required access to DDRS.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
73	System software changes are authorized, randomly sampled, and approved before implementation.	<u>DISA DECC-Ogden</u> All software changes and upgrades are approved, by either the DISA Change Control Board or the DISA DECC-Ogden Change Control Board, and are developed in a closed environment. All existing software or migrated software and firmware were thoroughly randomly sampled prior to installation on DISA DECC-Ogden's production platforms. Any new software undergoes the same testing procedures. If software vulnerabilities are identified, the commercial vendors, Government Central Design Agencies, or appropriate Systems Support Offices test, correct, and field appropriate patches or upgrades to correct the problem.	<u>DISA DECC-Ogden</u> Requested and inspected the change management policies and procedures for system software to confirm that they existed and were current.	<u>DISA DECC-Ogden</u> No relevant exceptions noted.
74	Installation of system software is documented and reviewed.	<u>DISA DECC-Ogden</u> Installation procedures for the Operating System are maintained within the DISA DECC-Ogden Business Continuity Plan.	<u>DISA DECC-Ogden</u> Inspected and read the DISA DECC-Ogden Business Continuity Plan to confirm that the installation of system software was documented and reviewed.	<u>DISA DECC-Ogden</u> No relevant exceptions noted.
75	Good engineering practices with regards to the integrity mechanisms of commercial-off-the-shelf, Government-off-the-shelf, and custom developed solutions are implemented for incoming and outgoing files.	<u>DISA DECC-Ogden</u> Policy mandates the use of Secure Socket Shell, Secure File Transfer Protocol, or Secure Communications Processor for file transfers.	<u>DISA DECC-Ogden</u> Confirmed through inquiry of the System Administrator that there were no automated system interfaces between DDRS and other automated information systems. Performed network monitoring and testing using the Securify	<u>DISA DECC-Ogden</u> The test results have been removed from the SAS 70 Report due to the sensitivity of the information contained in the test results.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>tool to confirm that no unencrypted traffic was transmitted over the DISA DECC-Ogden networks.</p> <p>Inspected and read the DDRS SSAA to confirm that no automated interfaces exist.</p>	
	<i>Segregation of Duties</i>			
76	<p>Incompatible duties have been identified and policies implemented to segregate these duties.</p>	<p><u>DISA DECC-Ogden</u> System Administration, System Security, Information Assurance Officer, and Information Assurance Manager duties are all separated at DISA DECC-Ogden.</p> <p>System Administrators manage server software and hardware. System Security Administrators manage weekly System Readiness Review scripts and manage all Information Assurance Vulnerability Alert requirements. DBAs manage databases and application support. Information Assurance Officers and Information Assurance Managers manage documentation for all findings, store auditing files, and do vulnerability scans.</p> <p><u>DFAS-Arlington</u> DDRS has a Program Manager, an Information Assurance Officer, Assistant Information Assurance Officers, and an Information Assurance Manager. Additionally, the DDRS software prohibits an individual from</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of DISA DECC-Ogden personnel and inspection of job descriptions that DISA had effectively segregated incompatible duties.</p> <p>Inspected the DISA DECC-Ogden organization chart to confirm that it existed, was current, and was approved by management.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Officer and inspection of job descriptions that DFAS-Arlington had effectively segregated incompatible duties.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>approving any transaction that they have initiated such as a Journal Voucher or a trial balance correction. In DDRS Budgetary, assignment of powerful roles like these are restricted to the “Headquarters System Security Administrator” role.</p> <p><u>DFAS-Cleveland</u> To define the guidelines and roles for the development and implementation of DDRS products, to this date, twenty two DDRS policies have been developed to ensure due process and repeatability in the interest of quality in the DDRS software process and its products. There is also a Software Quality Assurance function in place to ensure developers are following policies and procedures.</p> <p><u>DFAS-Indianapolis</u> The DDRS application is controlled by Oracle roles assigned to users. Managers oversee user access as documented on the SAAR form.</p>	<p>Read the DDRS PMO organizational chart and job descriptions to confirm that all positions were established in writing.</p> <p>Inspected the Appointment Letters for the Information Assurance Officer, Assistant Information Assurance Officer and the Information Assurance Manager to confirm that these individuals had been appointed in writing with the responsibilities of their positions included in the appointment letters.</p> <p><u>DFAS-Cleveland</u> Confirmed through inquiry of DFAS-Cleveland personnel and inspection of job descriptions that DFAS-Cleveland had effectively segregated incompatible duties.</p> <p>Read the DFAS-Cleveland organizational chart and job descriptions to confirm that all positions were established in writing.</p> <p><u>DFAS-Indianapolis</u> Confirmed through inquiry of DFAS-Indianapolis personnel and inspection of job descriptions that DFAS-</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			Indianapolis had effectively segregated incompatible duties. Read the DFAS-Indianapolis organizational chart and job descriptions to confirm that all positions were established in writing.	
77	System management job descriptions have been documented.	<p><u>DISA DECC-Ogden</u> All job descriptions are documented and stored at DISA DECC-Ogden.</p> <p><u>DFAS-Arlington</u> Job descriptions are reviewed on an annual basis in conjunction with establishing DFAS employee performance standards. After the award of a contract, the contractor is required to submit a Project Management Plan to state the approach to satisfying contract deliverables. This plan includes the job titles and descriptions of the staffing plan.</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of DISA DECC-Ogden personnel and inspection of job descriptions that DISA had effectively segregated incompatible duties.</p> <p>Inspected the DISA DECC-Ogden organization chart to confirm that it existed, was current, and was approved by management.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Officer and inspection of job descriptions that DFAS-Arlington had segregated incompatible duties.</p> <p>Read the DDRS PMO organizational chart and job descriptions to confirm that all positions were established in writing.</p> <p>Inspected the Appointment Letters for the Information</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Indianapolis</u> Job descriptions are documented for TSO personnel in the Mid-tier guidelines and procedures. Job responsibilities for the end users of the application are documented by the development staff in accordance with specifics outlined by the requirements documentation.</p>	<p>Assurance Officer, Assistant Information Assurance Officer and the Information Assurance Manager to confirm that these individuals had been appointed in writing with their responsibilities included in their appointment letters.</p> <p><u>DFAS-Indianapolis</u> Confirmed through inquiry of DFAS-Indianapolis personnel and inspection of job descriptions that DFAS-Indianapolis had segregated incompatible duties.</p> <p>Read the DFAS-Indianapolis organizational chart and job descriptions to confirm that all positions were established in writing.</p>	<p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>
78	System management employees understand their duties and responsibilities.	<p><u>DISA DECC-Ogden</u> All DISA DECC-Ogden employees understand their duties and responsibilities in accordance with DISA policies and procedures. Written position descriptions exist for all security personnel and all personnel are aware of their respective roles and responsibilities.</p> <p><u>DFAS-Arlington</u> Supervisors and employees discuss and sign performance standards for each employee. After the award of a contract, the contractor is required to</p>	<p><u>DISA DECC-Ogden</u> Inspected a random sample of three employees and confirmed through inquiry that they understood their duties and responsibilities and inspected documentation to confirm that employees had signed position descriptions.</p> <p><u>DFAS-Arlington</u> Inspected all 13 employees and confirmed through inquiry that they understood their duties and responsibilities and inspected</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>submit a Project Management Plan to state the approach to satisfy contract deliverables. This plan verifies the contractor's understanding of their duties.</p> <p><u>DFAS-Cleveland</u> Employees interviewed understand their primary job responsibility and are aware of documentation identifying their position description. Each position description identifies major duties, supervisory controls, and guidelines.</p> <p><u>DFAS-Indianapolis</u> The specific duties and responsibilities are part of the job descriptions each employee attests to when accepting the job. These duties and responsibilities are reviewed and managed by the Management Staff of the Configuration Management Information System</p>	<p>documentation to confirm that employees had signed position descriptions.</p> <p><u>DFAS-Cleveland</u> Inspected a random sample of 26 employees and confirmed through inquiry that they understood their duties and responsibilities and inspected documentation to confirm that employees had signed position descriptions.</p> <p><u>DFAS-Indianapolis</u> Inspected a random sample of eight employees and confirmed through inquiry that they understood their duties and responsibilities and inspected documentation to confirm that employees had signed position descriptions.</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>
79	Management reviews effectiveness of control techniques.	<p><u>DISA DECC-Ogden</u> As part of the DITSCAP process, the DISA DECC-Ogden Information Assurance Manger conducts and reviews the SSAA on an annual basis or when there is a major change. Additionally, Automated SRR scripts are run on each server and reported to the Montgomery SRR database on a weekly basis. Each system has SRR and an Information System Security scan</p>	<p><u>DISA DECC-Ogden</u> Read the latest risk assessment dated February 20, 2004 included in the DISA DECC-Ogden SSAA to confirm that risks were periodically assessed.</p> <p>Observed the SRR process to confirm that it occurred and that corrective actions were tracked.</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>before it is connected to the network. The DISA DECC-Ogden Field Security Office runs periodic SRRs and Information System Security scans.</p> <p><u>DFAS-Arlington</u> The DDRS application security risks are sampled and analyzed every three years. These risks are reported to DFAS Information Assurance management, and are considered for accreditation and re-accreditation every three years.</p>	<p>Inspected a single SRR performed by DISA DECC-Ogden and inspected the Vulnerability Management System findings report to confirm findings identified by the SRR process had been addressed.</p> <p><u>DFAS-Arlington</u> Read the latest risk assessment dated July 28, 2002 included in the DISA Ogden SSAA to confirm that risks were periodically assessed.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>
80	Formal procedures guide system management personnel in performing their duties.	<p><u>DISA DECC-Ogden</u> No formal procedures.</p> <p><u>DFAS-Arlington</u> Government employees follow their performance standards and Standard Operating Procedures (SOP) where appropriate. After the award of a contract, the contractor is required to submit a Project Management Plan to state the approach to satisfying contract deliverables. Contract staff is guided by this plan.</p> <p><u>DFAS-Cleveland</u> Each DDRS change management policy has a Roles and Responsibility section.</p>	<p><u>DISA DECC-Ogden</u> Read SOPs used by DISA DECC-Ogden personnel to confirm their DDRS-related job duties were documented.</p> <p><u>DFAS-Arlington</u> Read Standard Operating Procedures used by DFAS-Arlington personnel to confirm their DDRS-related job duties were documented.</p> <p><u>DFAS-Cleveland</u> Read Standard Operating Procedures used by DFAS-</p>	<p><u>DISA DECC-Ogden</u> SOPs and DISA DECC-Ogden SSAA were outdated and incomplete.</p> <p><u>DFAS-Arlington</u> Standard Operating Procedures were not available for review.</p> <p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>To achieve this objective, it has been declared mandatory for the DDRS Development Team to observe and adhere to Policies and Procedures in helping to dictate behavior and actions during the development process.</p> <p><u>DFAS-Indianapolis</u> The DBAs are governed by the policies and procedures outlined in the Mid-Tier Policy and Procedures.</p>	<p>Cleveland personnel to confirm their DDRS-related job duties were documented.</p> <p><u>DFAS-Indianapolis</u> Read Standard Operating Procedures used by DFAS-Indianapolis personnel to confirm their DDRS-related job duties were documented.</p>	<p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>
81	<p>Access procedures enforce the principles of separation of duties and “least privilege.”</p>	<p><u>DISA DECC-Ogden</u> Access to the DDRS Operating System is based on need-to-know access rules. All users must fill out the SAAR form and have a government official sign the form confirming need-to-know access.</p> <p><u>DFAS-Arlington</u> DDRS users have assigned user roles and organizational work areas that restrict their activities within datasets to what they need for their job duties.</p>	<p><u>DISA DECC-Ogden</u> Confirmed through inquiry of the DDRS System Administrator the process for obtaining an administrator account on the DDRS Operating System.</p> <p>Inspected all nine SAAR forms to confirm that a form was on file for all System Administrators with access to the DDRS Operating System.</p> <p><u>DFAS-Arlington</u> Confirmed through inquiry of the Information Assurance Officer the process for obtaining a user account on DDRS.</p> <p>Inspected all 18 SAAR forms to confirm that a form was on file</p>	<p><u>DISA DECC-Ogden</u> Seven of nine SAAR forms inspected did not have the signature of the Information Assurance Officer on the SAAR form.</p> <p>One System Administrator did not have a SAAR form on file. Additionally, access had not been removed for that user in a timely manner. This user’s access was subsequently deleted because he no longer required access to DDRS.</p> <p><u>DFAS-Arlington</u> Three of 18 SAAR forms did not document justification for access, and another three did not document type of system access.</p> <p>One of 22 CMIS PMO users had access to roles that were not</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Cleveland</u> Cleveland Management has identified and authorized CMIS, Project Version Control System (PVCS) and Oracle Versioning users and their access has been documented and approved.</p>	<p>for the DDRS PMO staff with access to DDRS.</p> <p>Inspected all 22 CMIS access forms to confirm that a form was on file for PMO staff with access to the CMIS.</p> <p><u>DFAS-Cleveland</u> Confirmed through inquiry of DDRS Configuration Manager, Project Version Control System (PVCS) Configuration Manager and DDRS Budgetary Module Team Lead the process for recording access to the CMIS, the PVCS, and the Oracle Versioning application.</p> <p>Inspected CMIS access forms to confirm that a form was on file for the 33 DDRS development staff with access to the CMIS.</p> <p>Inspected 6i Repository User Access Forms for a random sample of 31 DFAS-Cleveland DDRS staff members to confirm that a form was on file for the DDRS development staff with access to the Oracle Versioning System.</p> <p>Requested access forms to confirm that a form was on file for DDRS development staff with access to the PVCS.</p>	<p>required for his duties.</p> <p>Seven of 22 CMIS PMO users were former DDRS PMO staff, but their access to CMIS had not been terminated.</p> <p><u>DFAS-Cleveland</u> There were no forms used to track PVCS access.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p><u>DFAS-Indianapolis</u> The SAAR form documents the need for the individual to access the system. The developers define the roles required for the individual job responsibilities and the Oracle role is the catalyst for those permissions defined within the application. These roles are subsequently granted to the individual user when access to the application is granted.</p>	<p><u>DFAS-Indianapolis</u> Inquired of the DDRS Project Manager and the lead DBA of the process for granting the DBA access to DDRS.</p> <p>Inspected all six SAAR forms to confirm that a form was on file for the DBAs with access to DDRS.</p> <p>Inquired of the end user account administrator regarding DDRS end user account creation, modification, deletion, and password reset process.</p>	<p><u>DFAS-Indianapolis</u> One of six SAAR forms for DBAs did not have the justification for access completed on the SAAR form.</p> <p>None of the six SAAR forms inspected for DBAs had the signatures of the Functional Data Owner and Information Assurance Officer.</p> <p>One of six DBAs approved his own SAAR form.</p>
82	Active supervision and review are provided for all system management personnel.	<p><u>DISA DECC-Ogden</u> Personnel actions are reviewed by management structure of PMO Team Leads, Branch Chief, Division Chief, Deputy Director, and Director.</p> <p><u>DFAS-Arlington</u> The immediate and second level supervisors review and sign the performance standards and performance appraisals for all employees. Contractors provide status reports that are reviewed by the Program Manager. In addition, within the PMO,</p>	<p><u>DISA DECC-Ogden</u> Read the DISA DECC-Ogden organizational chart to confirm that a management structure was documented.</p> <p>Read position descriptions of DDRS support personnel to confirm supervisory responsibilities were documented.</p> <p><u>DFAS-Arlington</u> Read the DFAS-Arlington organizational chart to confirm that a management structure was documented.</p> <p>Read position descriptions of DDRS support personnel to</p>	<p><u>DISA DECC-Ogden</u> No relevant exceptions noted.</p> <p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>government employees and contract staff work as a team in close coordination with the program manager.</p> <p><u>DFAS-Cleveland</u> Every DFAS-Cleveland employee has a local supervisor that they report to. This supervisor performs annual performance reviews.</p> <p><u>DFAS-Indianapolis</u> Annual reviews are conducted for government employees by the employee's supervisor. The Federal Government conducts reviews of contractors.</p>	<p>confirm supervisory responsibilities were documented.</p> <p><u>DFAS-Cleveland</u> Read the DFAS-Cleveland organizational chart to confirm that a management structure was documented.</p> <p>Read position descriptions of DDRS support personnel to confirm supervisory responsibilities were documented.</p> <p><u>DFAS-Indianapolis</u> Read the DFAS-Indianapolis organizational chart to confirm that a management structure was documented.</p> <p>Read position descriptions of DDRS support personnel to confirm supervisory responsibilities were documented.</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p> <p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>

DDRS-Audited Financial Statements Module

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
1	<i>Financial Statements</i>			
	<p>Controls provide reasonable assurance that financial statements and related footnotes are produced in conformance with the reporting requirements of Financial Accounting Standards Advisory Board (FASAB), Office of Management and Budget (OMB) Bulletin No. 01-09, Form and Content of Agency Financial Statements (OMB Bulletin No. 01-09,) and the Department of the Treasury, Financial Management Service (Treasury.)</p> <p>Controls provide reasonable assurance that financial statements report all material financial information required by FASAB, Treasury and OMB, and that automated totals in the financial statements are appropriately calculated.</p>	<p>1. DoD Reporting policy ensures that the financial statements include all reportable items and related footnotes include all required disclosures in accordance with FASAB, OMB 01-09, and Treasury requirements.</p>	<p>Read DFAS policies pertaining to the preparation of financial statements and footnotes to determine whether they conformed to OMB, Treasury and FASAB reporting requirements.</p> <p>Compared the DoD financial statement footnotes appearing in FY 2004 Performance and Accountability Report to the Government Accountability Office’s “Checklist for Federal Accounting, Reporting and Disclosure” to determine whether footnotes included all required disclosures in accordance with FASAB, and OMB Bulletin No. 01-09.</p> <p>Analyzed DoD Fiscal Year 2005 Quarter 1 (FY 05 Q1) financial statements to determine whether issues identified in the DoD FY 04 financial statements were still valid at FY 05 Q1.</p> <p>Inspected the contents of the Confirmation Letter issued by the customer to signify the review and acceptance of the financial statements prepared by DFAS.</p>	<p><u>DFAS-Arlington</u> Policies related to the preparation of financial statements and footnote disclosures did not provide for the reporting and disclosure of accounting information required by the Federal Accounting Standards Advisory Board (FASAB) and Office of Management and Budget (OMB) Bulletin 01-09 as follows:</p> <ol style="list-style-type: none"> 1) The Statement of Net Cost was not presented by program. 2) The value of Property in hands of contractors was not reported. 3) Property Plant & Equipment requirements change for Statement of Federal Financial Accounting Standard 23 had not yet been implemented. 4) Trading Partner elimination amounts were not corroborated by the buyer entity. 5) The methodology used to value Deferred Maintenance was not disclosed in the footnotes. 6) The value of Heritage Assets, seized property, certain categories of operating materials and supplies, non-exchange custodial revenue, and restrictions pertaining to unobligated balances were not disclosed.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>Confirmed, through corroborative inquiry, that footnotes included all required disclosures in accordance with FASAB, and OMB Bulletin No. 01-09.</p>	
		<p>2. Templates are used to produce financial statements in conformance with United States Standard General Ledger (USSGL) -Supplement No. S2 of the Treasury Financial Manual. for the following statements:</p> <ol style="list-style-type: none"> 1) Balance Sheet. 2) Statement of Net Cost. 3) Statement of Changes in Net Position. 4) Statement of Budgetary Resources. 5) Statement of Financing. 6) Statement of Custodial Activity, when applicable. 	<p>Compared the DDRS-AFS financial statement templates, Chart of Accounts, and account attributes to the USSGL for consistency.</p> <p>Confirmed, through corroborative inquiry, that templates were used to produce financial statements and related footnotes in conformance with the USSGL.</p>	<p><u>DFAS-Arlington</u> A formal system was not in place to identify differences between the DDRS-AFS report maps with USSGL crosswalks, and the reasons for those differences.</p> <p>Furthermore, the mapping of accounts used for the preparation of the Statement of Custodial Activity did not conform to Treasury requirements, and accounts with the custodial attribute were improperly mapped to the Statement of Changes in Net Position.</p>
		<p>3. Automated totals are used within financial statement templates to ensure that financial statement sub-totals and totals are mathematically correct.</p>	<p>Recalculated the FY 04 DoD, consolidated financial statements subtotals and totals to determine whether line item amounts accurately summed to their respective subtotals and totals, and that consolidating statements summed to DoD-wide consolidated statements.</p> <p>Confirmed, through corroborative inquiry, that automated totals within the</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p> <p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>templates appropriately summarized the financial statement line items and that sub-totals and totals are mathematically correct.</p>	
		<p>4. DDRS-AFS system design and other related procedures ensure that footnote schedule totals agree to the applicable line items in the statements, and the associated narrative is properly reflected in the footnote disclosures.</p>	<p>Reviewed footnote editing process in DDRS-AFS to determine whether the final version of the narrative was carried forward to the financial statements.</p> <p>Inspected the DDRS-AFS generated "Footnote to Statement" reconciliation reports for differences between financial statement line items and footnote totals.</p> <p>Confirmed, through corroborative inquiry, that the footnote narrative prepared in DDRS-AFS is carried forward to the footnotes in the final version of the financial statements.</p>	<p><u>DFAS-Arlington</u> <u>DFAS-Cleveland</u></p> <p>Users could inadvertently overwrite the footnotes of another entity processed by the same DFAS center, or overwrite each other's footnote edits within the same entity. However, mitigating controls were in place because the footnote narratives were reviewed by the customer to ensure that the content of the footnote was complete as evidenced in the completed Standard Guidance Checklist and customer's issuance of the Confirmation Letter. Thus, the control activity and the associated mitigating controls supported the control objective.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>5. Reporting and accounting guidance is prepared by DFAS-Arlington and disseminated to DFAS Centers to ensure that staff receives adequate training on the use of DDRS-AFS, and maintain their knowledge of FASAB and DoD reporting requirements.</p>	<p>Inspected relevant policies, current FASAB reporting requirements, and relevant FASAB accounting treatments to determine whether they were included in the Quarterly Guidance.</p> <p>Obtained e-mail distribution lists to determine whether DFAS-Arlington distributed the Quarterly Guidance to DFAS centers.</p> <p>Confirmed, through corroborative inquiry, that the staff were adequately trained to maintain their knowledge of DDRS-AFS processes and FASAB reporting requirements.</p> <p>Confirmed, through corroborative inquiry, that DDRS-AFS communicated FASAB and reporting requirements.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>6. Procedures are implemented to ensure that DDRS-AFS financial statements are internally consistent and that the proper budgetary and proprietary accounting relationships are established.</p>	<p>Confirmed, through observation, that the DFAS centers:</p> <ul style="list-style-type: none"> - Prepared the reconciliation reports as required by DFAS-Arlington to ensure that financial statements are consistent and that the proper budgetary and proprietary relationships are established, - Explained unresolved reconciling items, and - Submitted explanations to DFAS-Arlington as required by the Quarterly Guidance. <p>Confirmed, through corroborative inquiry, that DDRS-AFS financial statements were consistent with that of the USSGL as published by the U.S. Treasury.</p>	<p><u>DFAS-Arlington</u> <u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>The reconciliation process frequently resulted in adjustments to force agreement between data sources rather than to facilitate an analysis of the differences at the transaction level. Secondly, a policy to provide feedback to the client so that erroneous data causing the reconciliation differences could be corrected was not in place.</p>
		<p>7. Prior to each reporting period or on a periodic basis, the DDRS-AFS Chart of Accounts and report maps are updated to reflect changes in the USSGL Chart of Accounts and financial statement crosswalks.</p>	<p>Confirmed, through corroborative inquiry with DFAS-Arlington management, that periodic reviews of the DDRS Chart of Accounts and report maps are performed.</p> <p>Confirmed, through corroborative inquiry, that prior to each reporting period or on a periodic basis, the USSGL was reviewed for changes applicable to the DDRS-AFS module Chart of Accounts.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>8. Controls ensure that the balances represented in the financial statements are based on the current reporting period.</p>	<p>Inspected the trial balance import sheet to determine if data checks were enabled to allow DDRS-AFS to confirm that the period for which trial balance information was being imported was the current reporting period.</p> <p>Confirmed, through corroborative inquiry, that the balances represented in the financial statements were based on the proper reporting period.</p>	<p><u>DFAS-Arlington</u> <u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>Information contained on the Microsoft Excel trial balance import sheets did not indicate the quarterly reporting period that the uploaded information pertained to. However, as a mitigating control, the local unique process to prepare balances for import into DDRS-AFS contained controls to ensure that the balances are being imported for the current reporting period. Additionally, variation analysis would detect an incorrect upload that was not related to the current period. Thus, the control activity and the associated mitigating control supported the control objective.</p>
		<p>9. DFAS procedures are implemented to ensure that the DDRS-AFS module's database is recalculated automatically or manually initiated prior to issuing the financial statements for the current reporting period.</p>	<p>Inspected database controls to determine whether a database recalculation was manually initiated in DDRS-AFS prior to issuing financial statements in the DDRS-AFS module.</p> <p>Confirmed, through corroborative inquiry, that a database recalculation was manually performed prior to issuing the financial statements for the current reporting period.</p>	<p><u>DFAS-Arlington</u> <u>DFAS-Cleveland</u></p> <p>Although the database recalculation was manually initiated in DDRS-AFS, there were no systematic controls to automatically perform the reconciliation prior to producing financial statements. However, a mitigating control was in place because each center periodically performed an entity level</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				recalculation and the PMO periodically performed an agency wide level recalculation.
		10. DDRS-AFS is programmed to ensure that trading partner eliminations are performed at the appropriate level (e.g. fund, component or agency wide) and that balances in the accounts that record trading partner activity are properly eliminated.	<p>Analyzed DDRS-AFS reports and screen shots to determine whether amounts appearing on trading partner import sheets were carried to the elimination column of the consolidating Balance Sheet and Statement of Net Cost.</p> <p>Confirmed, through corroborative inquiry, that trading partner eliminations were performed at the appropriate level and that balances in the accounts that record trading partner activity are properly eliminated.</p>	<p><u>DFAS-Arlington</u> <u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>No relevant exceptions noted.</p>
		11. DDRS-AFS applications controls are designed to ensure that the ending balances for the prior fiscal year become the beginning balances for the current fiscal year for all real accounts, and reporting in subsequent periods does not affect these balances unless proper authorization is granted.	<p>Inspected reconciliation reports that DFAS-Arlington required of DFAS centers for FY 04 and FY 05 Q1 to determine whether the reconciliation between Prior Year ending balances and Current Year beginning balances was performed and showed no differences between ending and beginning balances.</p> <p>Observed that balances for each quarter were cumulative and did not affect the beginning balance.</p>	<p>Although DFAS Centers periodically reviewed user access roles for appropriateness, some of the DFAS Centers had a questionable number of users assigned the HQSA role. Specifically:</p> <ul style="list-style-type: none"> - DFAS-Arlington had 13 users assigned the HQSA role. - DFAS-Denver had 10 users assigned the HQSA role. - DFAS-Columbus had 17 users assigned the HQSA. <p>However, as a mitigating control, the Centers periodically review the</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>Selected financial statement account line item balances and determined that the ending balance at FY 04 became the beginning balance for the next year.</p> <p>Selected a random sample of DFAS-AFS users to determine if System Authorization Access Request (SAAR) forms matched the access provided.</p> <p>Inspected a list of DDRS-AFS users assigned the beginning balance modification role, and the Headquarters Security Administrator (HQSA) role, to determine whether this access was appropriate for their job responsibilities. HQSA is a powerful role that, while necessary on a limited basis, does not encompass the principles of separation of duties and least privilege.</p> <p>Inspected e-mail traffic to confirm that DFAS Centers periodically review user access for appropriateness.</p> <p>Confirmed, through corroborative inquiry, that the ending balances at FY 04 became the beginning balances for the next year, and that balances could not be altered</p>	<p>user access roles to determine if access is appropriate.</p> <p>Out of 162 total SAAR forms tested for all DDRS-AFS users, eight related to users of the DDRS_CFO_BEGINNING_BAL role which provides users with this role the ability to adjust beginning balances in DDRS-AFS. Of these eight users:</p> <ul style="list-style-type: none"> - Six users had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or DFAS center to which access should be granted. - One user had a post 2004 SAAR form on file, but the specific role did not exist on the SAAR form. - One user had a post 2004 SAAR form on file, but the specific role was not indicated on the form. <p>Out of 162 total SAAR forms tested for all DDRS-AFS users, 12 related to users of the DDRS_CFO_HQSA role which provides users with this role the ability to assign and remove roles in DDRS-AFS. Of these 12 users:</p> <ul style="list-style-type: none"> - Nine users had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or DFAS center to which access should be granted;

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			without authorization.	<p>- Two users had a post 2004 SAAR form on file, but the DDRS-AFS role granted on the form did not match access provided in DDRS-AFS; and,</p> <p>- One user did not have a SAAR form available.</p> <p>However, DFAS Centers periodically reviewed user access roles but did not determine whether these 12 HQSA users were appropriate.</p> <p><u>DFAS-Arlington</u> Out of 24 users with the beginning balance modification role, 23 of them did not require this role to perform their job responsibilities. The SAAR form used for DDRS-AFS prior to 2004 did not include specific role categories for which a user had been authorized.</p> <p><u>DFAS-Denver</u> A systems developer was assigned access to the production environment as a HQSA, which creates segregation of duties risks. The HQSA role can add, change, and delete information.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>12. The design of DDRS-AFS in conjunction with manual procedures ensures that the FACTS 1 file submitted to Treasury is consistent with the amounts reported in the financial statements.</p>	<p>Recalculated financial statement line items using the data in the FACTS 1 file submitted to Treasury for FY 04 to determine whether the file agreed to the financial statements.</p> <p>Confirmed, through corroborative inquiry, that the FY 04 FACTS 1 file submitted to Treasury was consistent with the FY04 financial statements.</p>	<p><u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>Management did not sign-off on the FACTS 1 file or on the Treasury confirmation of a successful upload as evidence that a review was performed before or after submission to Treasury. Additionally, DDRS-AFS produced an incorrect Treasury symbol for DoD Working Capital Funds and personnel had to manually change the text file before transmission. At DFAS-Denver, however, as a mitigating control, personnel ensured that the text file balanced before transmission to Treasury, and they maintained the Treasury confirmation of a successful upload in their records.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>13. The DDRS-AFS generated Statement of Budgetary Resources is reconciled to the Report on Budget Execution and Budgetary Resources (SF-133) to ensure that DDRS-AFS is in agreement with the budgetary system which prepares the SF-133 on a monthly basis.</p>	<p>Inspected the series of reconciliation reports that DFAS-Arlington requires of DFAS centers for FY 04 and FY 05 Q1 to determine whether the reconciliation between Statement of Budgetary Resources and Report on Budget Execution and Budgetary Resources (SF-133.) was performed and differences were explained.</p> <p>Confirmed, through corroborative inquiry, that the Statement of Budgetary Resources is reconciled to the Report on Budget Execution and Budgetary Resources (SF-133) to ensure that DDRS-AFS is in agreement with the budgetary system, which prepares the SF-133 on a monthly basis.</p>	<p><u>DFAS-Arlington</u> <u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>Although the SF-133 and Statement of Budgetary Resources reconciliation was performed, management did not sign off on the reconciliation reports evidencing a review before they were submitted to DFAS-Arlington.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
2	<i>Audit Trails</i>			
	<p>Controls provide reasonable assurance that DDRS-AFS produces financial statements that are supported by audit trails that are adequate for the financial management entity and external auditors to trace amounts reported in the financial statement back to trial balances and data from feeder systems. Controls provide reasonable assurance that audit trails indicate the user inputting the trial balance and the user approving the trial balance. All audit trails indicate the user inputting the Journal Voucher and the user approving the Journal Voucher. Audit trails are reviewed on a regular basis for appropriateness.</p>	<p>1. DDRS-AFS has the capability to allow users to view the components of financial statement line items at the various levels of consolidation – from the reporting “entity” level to the “program” level where information is originally input.</p>	<p>Used hyperlinks embedded in the DDRS-AFS final trial balance supporting the financial statements to view and trace the components of line items, including Journal Voucher adjustments, from the entity level of consolidation back to the program level where trial balance was originally entered either manually or uploaded using “import sheets” created in Microsoft Excel.</p> <p>Confirmed, through corroborative inquiry, that components of financial statement line item amounts may be viewed at the entity, sub-entity, program group, and program level.</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted</p>
		<p>2. Balances entered into DDRS-AFS either (1) manually, or (2) imported via Microsoft Excel import sheets, or (3) imported from the Data Collection Module (DCM) are supported by system audit trails.</p>	<p>Obtained a random sample of trial balance upload system audit trails to determine whether they contained username, date, and time of uploads into DDRS-AFS.</p> <p>Confirmed, through corroborative inquiry, that balances entered into DDRS-AFS (1) manually, or (2) imported via Microsoft Excel import sheets, or (3) imported from the DCM, are supported by systems audit trails.</p>	<p><u>DFAS-Cleveland</u> Although trial balance deletions were recorded in the audit log with a date, time, and user ID, there was no entry in the log indicating the original deleted trial balance amounts.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>3. Journal Vouchers entered into DDRS-AFS are supported by audit trails indicating (1) the User ID entering the Journal Voucher (2) the User ID approving the journal, and (3) the date and time when the Journal Voucher was entered and posted.</p>	<p>Inspected the Journal Voucher system audit log in DDRS-AFS to determine whether Journal Vouchers were supported by audit trails indicating the User ID entering the Journal Voucher and the User ID approving the Journal Voucher, and the dates and times of entry and approval.</p> <p>Confirmed, through corroborative inquiry, that Journal Vouchers entered in DDRS-AFS were supported by audit trails indicating the User ID entering the Journal Voucher, the User ID approving the Journal Voucher, and the dates and times of entry and approval.</p>	<p><u>DFAS-Cleveland</u> An audit trail was not established for Journal Vouchers which were deleted as a part of the trial balance deletion function. Additionally, the audit trail for cancelled Journal Vouchers did not display the user who performed the cancellation, nor the date or reason for the cancellation. Lastly, the DDRS Journal Voucher log which was exported into Microsoft Excel for analysis did not accurately display the Journal Voucher approval identification, although the Journal Voucher unique identifier control number was correctly displayed. However, as a mitigating control, the approval identification displayed properly in Microsoft Word and Adobe Acrobat. Thus, the control activities and the associated mitigating controls supported the control objective.</p>
		<p>4. Audit trails in DDRS-AFS are periodically reviewed for appropriateness and unusual activity on a quarterly basis.</p>	<p>Inspected audit trails at each center to determine whether signoffs existed to confirm audit trails were reviewed.</p> <p>Confirmed, through corroborative inquiry that, audit trails in DDRS-AFS were reviewed for appropriateness and unusual activity on a quarterly basis.</p>	<p><u>DFAS-Cleveland</u> <u>DFAS-Columbus</u> <u>DFAS-Indianapolis</u> <u>DFAS-Denver</u></p> <p>System audit logs are not regularly reviewed. Secondly, a report which would facilitate a review of the audit log pertaining to footnote uploads was not implemented during the period covered by our testwork but was subsequently</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				implemented in March. However, we were unable to confirm that the footnote audit logs were reviewed in the reporting period following their implementation.
		5. Deleted trial balances and associated deleted Journal Vouchers are recorded with the User ID, date, and time they were deleted.	<p>Inspected trial balance deletion logs to determine whether deleted trial balances and deleted journal entries were recorded with the User ID, date and time deleted.</p> <p>Confirmed, through corroborative inquiry, that all deleted trial balances and associated journal entries were recorded with the User ID, date and time deleted.</p>	<u>DFAS-Cleveland</u> DDRS-AFS did not maintain a history of the detail of trial balance deletions and the associated deleted Journal Vouchers that may have been posted to the trial balance prior to deletion.
3	<i>Journal Vouchers</i>			
	Controls provide reasonable assurance that Journal Vouchers are: - supported by adequate documentation, and approved prior to entry into a DDRS-AFS table; - processed with the duties of preparation and approval being properly segregated; and, - in balance prior to entry into DDRS.	1. Procedures are in place to ensure that the Journal Voucher package is reviewed for adequacy and approved prior to entry into DDRS-AFS.	<p>Selected a random sample of Journal Vouchers to determine whether they were supported by adequate documentation and, approved prior to entry into DDRS-AFS.</p> <p>Confirmed, through corroborative inquiry, that Journal Vouchers were reviewed for adequate documentation, and approved prior to entry into DDRS-AFS.</p>	<p><u>DFAS-Arlington</u> <u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>Adherence to the FMR Journal Voucher approval policy was inconsistent across the DFAS centers. DFAS Directors were designated by the FMR to approve Journal Vouchers in excess of one billion dollars. Although Journal Voucher packages were reviewed by management before entry into DDRS-AFS, the FMR requirement</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				<p>that Journal Vouchers in excess of one billion dollars be specifically approved by the Director prior to entry was not always adhered to in a timely manner.</p> <p>C, I, and E categories of Journal Vouchers which facilitate agreement between the financial statements and internal or external reports, or to facilitate proper trading partner elimination, were not supported by a transaction level analysis. Thus, the amounts appearing in the Journal Voucher were mainly differences between select line items in the statements at the reporting level, or a simple adjustment of buyer side data to seller-side data without reconciliation between both buyer and seller data.</p>
		<p>2. User roles are established to ensure that Journal Vouchers are approved by an individual other than who is entering the Journal Voucher and who has authority to approve the Journal Voucher and the ability to enter or modify information contained in a Journal Voucher is restricted to authorized personnel.</p>	<p>Selected a random sample of DFAS-AFS users to determine if SAAR forms matched the access provided.</p> <p>Inspected a list of DDRS-AFS users assigned the Journal Voucher approver role, and the HQSA role, to determine whether this access was appropriate for their job responsibilities. HQSA is a powerful role that, while necessary on a limited basis, does not encompass the</p>	<p>Although DFAS Centers periodically reviewed user access roles for appropriateness, some of the DFAS Centers had a questionable number of users assigned the HQSA role. Specifically:</p> <ul style="list-style-type: none"> - DFAS-Arlington had 13 users assigned the HQSA role. - DFAS-Denver had 10 users assigned the HQSA role. - DFAS-Columbus had 17 users assigned the HQSA role.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>principles of separation of duties and least privileges.</p> <p>Inspected e-mail traffic to confirm that DFAS Centers periodically review user access for appropriateness.</p> <p>Inspected DDRS-AFS system audit logs and system controls to determine whether users could approve their own Journal Vouchers.</p> <p>Confirmed, through corroborative inquiry, that Journal Vouchers were approved by an individual other than the individual who entered the Journal Voucher.</p> <p>Confirmed, through corroborative inquiry, that the ability to enter or modify information contained in a Journal Voucher was restricted to authorized personnel.</p>	<p>Controls were designed to provide for access to DDRS-AFS on a center-level basis, instead of by responsible work area. As such, the user may have access to information that they don't necessarily need.</p> <p>Out of 162 total SAAR forms tested for all DDRS-AFS users, 27 related to users of the DDRS_CFO_JV_CREATOR role which provides users with this role the ability to create Journal Vouchers in DDRS-AFS. Of these 27 users:</p> <ul style="list-style-type: none"> - Ten users had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or DFAS center to which access should be granted; - Ten users had a post 2004 SAAR form on file, but the specific role was not indicated on the form; - One user had a post 2004 SAAR form on file, but the DDRS-AFS role granted on the form did not match access provided in DDRS-AFS and, - Two users were missing one or more required signatures. <p>However, DFAS Centers periodically reviewed user access roles for appropriateness.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				<p>Out of 162 total SAAR forms tested for all DDRS-AFS users, 19 related to users of the DDRS_CFO_JV_APPROVER roles which provide users with these roles the ability to approve Journal Vouchers at different levels in DDRS-AFS. Of these 19 users:</p> <ul style="list-style-type: none"> - Nine users had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or DFAS center to which access should be granted; - One user had a post 2004 SAAR form on file, but the specific role did not exist on the SAAR form; - One user had a post 2004 SAAR form on file, but the specific role was not indicated on the form; and, - Two users had a post 2004 SAAR form on file, but the DDRS-AFS role granted on the form did not match access provided in DDRS-AFS. <p>However, DFAS Centers periodically reviewed user access roles for appropriateness.</p> <p>Out of 162 total SAAR forms tested for all DDRS-AFS users, 12 related to users of the DDRS_CFO_HQSA role which provides users with this role the ability to assign and remove roles in DDRS-AFS. Of these 12 users:</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				<p>- Nine users had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or DFAS center to which access should be granted.</p> <p>- Two users had a post 2004 SAAR form on file, but the DDRS-AFS role granted on the form did not match access provided in DDRS-AFS.</p> <p>- One user did not have a SAAR form available.</p> <p>However, DFAS Centers periodically reviewed user access roles for appropriateness, but did not determine whether these 12 HQSA users were appropriate.</p> <p><u>DFAS-Arlington</u> The DDRS-AFS SAAR form used prior to 2004 did not include specific role categories for which a user had been authorized.</p> <p><u>DFAS-Denver</u> A systems developer was assigned access to the production environment as a HQSA, which creates segregation of duties risks.</p> <p>At DFAS-Denver, there are two individuals with a high dollar value Journal Voucher approval authority inconsistent with internal guidance provided by the Center. However, as a mitigating control,</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				the Journal Vouchers were approved by an appropriate individual.
		3. DDRS-AFS application controls prevent the processing of out-of balance Journal Vouchers, and notify the user of the out-of -balance condition with an error message.	<p>Observed that an attempt to enter an out-of-balance Journal Voucher was unsuccessful and resulted in an error message being displayed notifying the user of the out-of- balance condition.</p> <p>Confirmed, through corroborative inquiry, that DDRS-AFS will not process out-of-balance Journal Vouchers.</p>	<u>DFAS-Cleveland</u> No relevant exceptions noted.
		4. DDRS-AFS is designed to ensure that Journal Vouchers entered into DDRS-AFS are included in the intended reporting period.	<p>Reviewed Journal Voucher input process to determine whether Journal Vouchers can only be input for the current period.</p> <p>Traced certain Journal Vouchers through DDRS-AFS to determine whether the Journal Vouchers update the financial statements.</p> <p>Confirmed, through corroborative inquiry, that the Journal Vouchers entered into DDRS-AFS were included in the intended reporting period.</p>	<u>DFAS-Cleveland</u> No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>5. DDRS-AFS is designed so that Journal Vouchers, entered into DDRS-AFS, update all applicable general ledger account balances (i.e., budgetary, proprietary and memorandum accounts) and are included in the final trial balance numbers.</p>	<p>Selected a random sample of Journal Vouchers entered into DDRS-AFS to determine whether they updated applicable general ledger account balances and were included in the final trial balance numbers.</p>	<p><u>DFAS-Arlington</u> Two out of forty-five Journal Vouchers selected could not be traced to the correct trial balance and USSGL account because, according to the DFAS-Arlington PMO, the server responsible for generating the view of the trial balance and voucher being tested was not functioning properly and was not repaired before our testing concluded.</p>
		<p>6. DDRS-AFS PMO enables a lock-out mechanism to ensure that no adjustments are made to the trial balance subsequent to the submission of the financial statements to OMB.</p>	<p>Inspected the system audit log indicating the lockout occurred and observed that the lockout mechanism was enabled prior to the release of the statements to OMB, and that the mechanism was effective in preventing additional adjustments to the financial statements.</p> <p>Confirmed, through corroborative inquiry, that the DDRS-AFS PMO enables a lock-out mechanism to ensure that no adjustments were made to the trial balance subsequent to the submission of the financial statements to OMB.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>7. DDRS-AFS assigns control numbers in sequence to uniquely identify Journal Vouchers, and produces a sequentially ordered Journal Voucher log which can be used to identify missing vouchers and facilitate research.</p>	<p>Inspected the Journal Voucher log to determine whether it was sequentially ordered and, if breaks in the sequence of control numbers existed, whether they were explained.</p> <p>Confirmed, through corroborative inquiry, that missing Journal Voucher entries are identified by inspecting the sequence of control numbers assigned to Journal Vouchers by DDRS-AFS.</p>	<p><u>DFAS-Cleveland</u> Inspection of the Journal Voucher log showed that some numbers were missing from the sequence of Journal Voucher numbers as a result of a trial balance and associated Journal Vouchers being deleted. Additionally, the log did not accurately display a Journal Voucher identification number due to a programming error when exported into Microsoft Excel.</p>
		<p>8. Controls ensure that one-sided Budgetary and one-sided Proprietary transactions cannot occur.</p>	<p>Observed processing in DDRS-AFS to determine whether one-sided Budgetary and one-sided Proprietary transactions resulted in an error message and that processing cannot continue.</p> <p>Confirmed, through corroborative inquiry, that debits equal credits for the Proprietary and Budgetary accounts being posted.</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
4	<i>Trading Partners</i>			
	<p>Controls are in place to ensure that trading partner data are supported by adequate documentation or valid estimating methodology. Controls provide reasonable assurance that DDRS-AFS has systems or processes for determining the quality and integrity of data flowing through the system, and trading partners are input and updated completely and accurately. Reports can identify the impact of trading partners on statement presentation.</p>	<p>1. Seller initiated trading partner eliminations are automatically e-mailed by DDRS-AFS or otherwise provided the buyer and confirmed for appropriateness.</p>	<p>Obtained a random sample notification e-mail from DDRS-AFS displaying trading partner notification.</p> <p>Confirmed, through corroborative inquiry, that seller initiated trading partner eliminations were automatically e-mailed to the customer and approved for elimination amounts.</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p>
		<p>2. DDRS-AFS ensures that trading partner data input is subject to data checks to ensure that invalid information (erroneous USSGL Attribute combinations or erroneous trading partner identifier) was not allowed to process.</p>	<p>Observed system controls to determine whether only valid accounts updated DDRS-AFS tables.</p> <p>Confirmed, through corroborative inquiry, that DDRS-AFS trading partner data input was subject to data checks to ensure that invalid information (erroneous USSGL Attribute combinations or erroneous trading partner identifier) was not allowed to process.</p>	<p><u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u> No relevant exceptions noted.</p>
		<p>3. DFAS-Arlington PMO enables the DDRS-AFS “Lock-out” mechanism to ensure that trading partner information is not changed once the financial statements are finalized.</p>	<p>Inspected the system audit log indicating the lockout mechanism occurred and to determine whether entries could be made once the mechanism was enabled.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			Confirmed, through corroborative inquiry, that a mechanism existed to ensure that trading partner information could be locked down to prevent changes once the financial statements were finalized.	
		4. Significant policies and procedures are documented.	<p>Inspected policies and procedures to determine whether significant policies and procedures were documented.</p> <p>Confirmed, through corroborative inquiry, that significant policies and procedures were documented.</p>	<p><u>DFAS-Arlington</u> Review of the FMR and DFAS policies disclosed that the process of relying on seller-side data did not include a control for reconciling differences between seller and buyer data. Thus, the adjustments to buyer side accounts may not be auditable and material amounts of such adjustments could impact on the result of a financial statement audit.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
5	<i>Validation</i>			
	Controls provide reasonable assurance that DDRS-AFS has systems or processes for determining the quality and integrity of data flowing through the system, and trial balances are input and updated completely and accurately. Controls provide reasonable assurance that data validation and editing are performed to identify erroneous data, and that erroneous data are captured, reported, investigated, and corrected.	1. Control totals over data entered directly into DDRS-AFS ensure the trial balance or journal entry is in balance prior to updating DDRS-AFS.	<p>Observed trial balance entry to determine whether control totals over data entered directly into DDRS-AFS ensured the trial balance or journal entry was in balance prior to updating DDRS-AFS.</p> <p>Confirmed, through corroborative inquiry, that control totals over data entered directly into DDRS-AFS ensured the trial balance or journal entry was in balance prior to updating DDRS-AFS.</p>	<u>DFAS-Cleveland</u> No relevant exceptions noted.
		2. Control totals over data imported from an Excel sheet to text file into DDRS-AFS ensure the trial balance is in balance prior to updating DDRS-AFS.	<p>Observed the trial balance data import process to determine whether control totals in the import sheets ensured that the trial balance was in balance prior to updating DDRS-AFS.</p> <p>Confirmed, through corroborative inquiry, that control totals over data imported from an Excel sheet to text file into DDRS-AFS ensured the trial balance was in balance prior to updating DDRS-AFS.</p>	<u>DFAS-Cleveland</u> No relevant exceptions noted.
		3. Validation ensures abnormal balances are flagged for review at the line item level.	Inspected reports to determine whether non-traditional debit and credit accounts were flagged for review.	<u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>Inspected the customer's concurrence that abnormal balances (if any) had been identified and disclosed in the footnotes by verifying that the customer provided a "yes" response to the Standard Guidance Checklist item pertaining to abnormal balances.</p> <p>Confirmed, through corroborative inquiry, that validation ensured non-traditional debit and credit accounts were flagged for review.</p>	No relevant exceptions noted.
		4. Subsequent to importing trial balances, Journal Vouchers changes or adjustments to trial balances are reviewed and approved by management prior to report generation.	<p>Selected a random sample of Journal Vouchers to determine that any Journal Vouchers changes or adjustments to trial balances were reviewed and approved by management prior to report generation.</p> <p>Obtained a random sample of trial balance upload system audit trails to determine whether trial balance uploads contain an approval.</p> <p>Confirmed, through corroborative inquiry, that subsequent to trial balance import any Journal Vouchers changes or adjustments to trial balances were reviewed and</p>	<p><u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>Adherence to the FMR Journal Voucher approval policy was inconsistent across DFAS centers. Trial balance corrections entered into DDRS-AFS did not always require approval prior to posting, the ability to post Journal Vouchers was delegated to several staff accountants, and DFAS Directors did not always approve Journal Vouchers in excess of one billion dollars prior to posting. DFAS Directors were designated by the FMR to approve Journal Vouchers in excess of one billion</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			approved by management prior to report generation.	dollars. Although Journal Voucher packages were reviewed by management before entry into DDRS-AFS, the FMR requirement that Journal Vouchers in excess of one billion dollars be specifically approved by the Director prior to entry was not always adhered to in a timely manner.
		5. Variance analysis is performed to explain fluctuations between the current year and prior year amounts reported on the financial statements.	<p>Confirmed, through observation, that variation analyses were performed, and disclosure was made of the causes of variations greater than 10% from the previous year.</p> <p>Obtained variance analyses performed by DFAS personnel and confirmed that variances were explained and disclosed according to the FMR. Obtained the Standard Guidance Checklist and noted the customer's response to the associated checklist item on variance analysis.</p>	<p><u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>No relevant exceptions noted.</p>
		6. Standard programmed algorithms perform significant financial statement calculations.	Recalculated the FY 04 DoD consolidated financial statements subtotals and totals to determine whether line item amounts accurately sum to their respective subtotals and totals, and that consolidating statements summed to DoD-wide consolidated statements.	<p><u>DFAS-Cleveland</u></p> <p>No relevant exceptions noted</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			Confirmed, through corroborative inquiry, that standard programmed algorithms performed significant trial balance calculations.	
		7. Journal vouchers are automatically assigned a unique sequence number to facilitate their identification in the DDRS-AFS.	<p>Inspected a listing of Journal Voucher transaction IDs (control numbers) to determine whether they were assigned a unique sequence number.</p> <p>Confirmed, through corroborative inquiry, that transactions were automatically assigned a unique sequence number</p>	<p><u>DFAS-Cleveland</u> The Journal Vouchers were observed to be sequentially numbered; however, there were missing numbers in the series as a result of trial balance and associated Journal Voucher deletions which were not maintained in the history file. Additionally, the DDRS-AFS Journal Voucher log which was exported into Microsoft Excel for analysis did not accurately display the Journal Voucher approval identification, although the Journal Voucher unique identifier control number was correctly displayed. However, as a mitigating control, the approval identification displayed properly in Microsoft Word and Adobe Acrobat. Thus, the control activities and the associated mitigating controls supported the control objective.</p>
		8. The Microsoft Excel spreadsheets provided to reporting activities to use for importing trial balances into DDRS-AFS contain preprogrammed fields and totals to ensure data validation.	Inspected Microsoft Excel import sheets provided to reporting activities to determine whether the spreadsheets contained preprogrammed fields and totals to ensure data validation.	<p><u>DFAS-Cleveland</u> <u>DFAS-Columbus</u></p> <p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			Confirmed, through corroborative inquiry, that the Excel spreadsheets provided to reporting activities contained preprogrammed fields and totals to ensure data validation.	
		9. Trial balances and trading partner elimination entries imported into DDRS-AFS using Microsoft Excel files in CSV format update the proper accounts and tables.	<p>Traced trial balance account balances from the trading partner import sheet to the DDRS-AFS trial balance.</p> <p>Selected a random sample of trial balances imported into DDRS-AFS using a Microsoft Excel spreadsheet to determine whether the balance imported matched the resulting trial balance appearing in DDRS-AFS.</p> <p>Confirmed, through corroborative inquiry, that files imported in CSV format were imported into the proper accounts and tables.</p>	<p><u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>No relevant exceptions noted.</p>
		10. Reconciliations are performed to determine the reliability of data in the system and reconciling differences are identified and resolved.	Confirmed, through observation, that the DFAS centers: - prepared the reconciliation reports as required by DFAS-Arlington to ensure that financial statements are consistent and that the proper budgetary and proprietary relationships are established; - explained unresolved	<p><u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>The reconciliation process was used primarily to force agreement between statements. A process to provide feedback to the client was not in place to clear differences.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			reconciling items; and - submitted explanations to DFAS-Arlington as required by the Quarterly Guidance.	
6	<i>Authorized Trial Balance Entry</i>			
	<p>Controls provide reasonable assurance that data transmissions between DDRS-AFS and user organizations are authorized, complete, accurate, and secure.</p> <p>Unbalanced trial balances are flagged and not reported until in balance.</p> <p>Controls provide reasonable assurance that application users are appropriately identified and authenticated, and that access to the application and output is restricted to authorized users for authorized purposes.</p> <p>Controls provide reasonable assurance that trial balance input is accurate and recorded in the proper period.</p>	<p>1. Trial balance import sheets are input by authorized personnel.</p>	<p>Selected a random sample of DFAS-AFS users to determine if SAAR forms matched the access provided.</p> <p>Inspected a list of DDRS-AFS users assigned the data administrator role, and the HQSA role, to determine whether this access was appropriate for their job responsibilities. HQSA is a powerful role that, while necessary on a limited basis, does not encompass the principles of separation of duties and least privileges.</p> <p>Inspected e-mail traffic to confirm that DFAS Centers periodically review user access for appropriateness.</p> <p>Confirmed, through corroborative inquiry, that trial balance import sheets were input by authorized personnel.</p>	<p>Controls were designed to provide for access to DDRS-AFS on a center-level basis, instead of by responsible work area. As such, the user may have access to information that they don't necessarily need.</p> <p>Out of 162 total SAAR forms tested for all DDRS-AFS users, five related to users of the DDRS_CFO_DATA_ADMIN role which provides users with this role the ability to import and edit trial balances in DDRS-AFS. Of these five users:</p> <ul style="list-style-type: none"> - One user had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or DFAS center to which access should be granted. - Two users had a post 2004 SAAR form on file, but the DDRS-AFS role granted on the form did not match access provided in DDRS-AFS. <p>However, DFAS Centers periodically reviewed user access roles for appropriateness.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				<p>Out of 162 total SAAR forms tested for all DDRS-AFS users, 12 related to users of the DDRS_CFO_HQSA role which provides users with this role the ability to assign and remove roles in DDRS-AFS. Of these 12 users:</p> <ul style="list-style-type: none"> - Nine users had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or DFAS center to which access should be granted. - Two users had a post 2004 SAAR form on file, but the DDRS-AFS role granted on the form did not match access provided in DDRS-AFS. - One user did not have a SAAR form available. <p>However, DFAS Centers periodically reviewed user access roles for appropriateness, but did not determine whether these 12 HQSA users were appropriate.</p> <p>Although DFAS Centers periodically reviewed user access roles for appropriateness, some of the DFAS Centers had a questionable number of users assigned the HQSA role. Specifically:</p> <ul style="list-style-type: none"> - DFAS-Arlington had 13 users assigned the HQSA role. - DFAS-Denver had 10 users assigned the HQSA role.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				<p>- DFAS-Columbus had 17 users assigned the HQSA role.</p> <p><u>DFAS-Arlington</u> The DDRS-AFS SAAR form used prior to 2004 did not include specific role categories for which a user had been authorized.</p> <p><u>DFAS-Cleveland</u> The import sheets uploaded into DDRS did not require approval prior to posting.</p> <p>The trial uploads and balance adjustments entered into DDRS-AFS did not require approval prior to posting.</p> <p><u>DFAS-Denver</u> A systems developer in Cleveland was assigned access to the production environment as a HQSA, which creates segregation of duties risks.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>2. Microsoft Excel trial balance import sheets received by reporting activities are complete and in balance.</p>	<p>Randomly sampled Microsoft Excel trial balances at 2004 FYE and at 2005 1QE to determine whether Microsoft Excel trial balance import sheets, budgetary import sheets, and trading partner import sheet transmissions received by reporting activities were complete and in balance.</p> <p>Confirmed, through corroborative inquiry, that Microsoft Excel trial balance import sheets, budgetary import sheets, and trading partner import sheet transmissions received by reporting activities were complete and in balance.</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p>
		<p>3. DDRS-AFS design establishes separate roles for Trial Balance import, Trial Balance validation, and Trial Balance reconciliation.</p>	<p>Inspected system roles to determine if Trial Balance Import, Trial Balance Validation, and Trial Balance Reconciliation were defined as separate roles in DDRS-AFS.</p> <p>Confirmed, through corroborative inquiry, that the system had separate roles identified for Trial Balance import, Trial Balance validation and Trial Balance reconciliation.</p>	<p><u>DFAS-Cleveland</u> Trial Balance approval roles were not established in DDRS-AFS.</p>
		<p>4. Direct trial balance entries into DDRS-AFS or edits to the trial balance are performed by the appropriate reporting activities and are from authorized personnel at the activity.</p>	<p>Selected a random sample of DFAS-AFS users to determine if SAAR forms matched the access provided.</p>	<p>Controls were designed to provide for access to DDRS-AFS on a center-level basis, instead of by responsible work area. As such, the user may have access to</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>Inspected a list of DDRS-AFS users assigned the Journal Voucher approver role and the HQSA role to determine whether this access was appropriate for their job responsibilities. HQSA is a powerful role that, while necessary on a limited basis, does not encompass the principles of separation of duties and least privileges.</p> <p>Inspected e-mail traffic to confirm that DFAS Centers periodically review user access for appropriateness.</p> <p>Confirmed users with ability to upload trial balances by obtaining the SAAR form and confirming that the user was authorized to upload balances.</p> <p>Confirmed, through corroborative inquiry, that direct trial balance entries into DDRS-AFS or edits to the trial balance were performed by the appropriate reporting activities and were from authorized personnel at the activity.</p>	<p>information that they don't necessarily need.</p> <p>Out of 162 total SAAR forms tested for all DDRS-AFS users, five related to users of the DDRS_CFO_DATA_ADMIN role which provides users with this role the ability to import and edit trial balances in DDRS-AFS. Of these five users:</p> <ul style="list-style-type: none"> - One user had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or DFAS center to which access should be granted: - Two users had a post 2004 SAAR form on file, but the DDRS-AFS role granted on the form did not match access provided in DDRS-AFS. <p>However, DFAS Centers periodically reviewed user access roles for appropriateness</p> <p>Out of 162 total SAAR forms tested for all DDRS-AFS users, 12 related to users of the DDRS_CFO_HQSA role which provides users with this role the ability to assign and remove roles in DDRS-AFS. Of these 12 users:</p> <ul style="list-style-type: none"> - Nine users had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or DFAS

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				<p>center to which access should be granted.</p> <ul style="list-style-type: none"> - Two users had a post 2004 SAAR form on file, but the DDRS-AFS role granted on the form did not match access provided in DDRS-AFS. - One user did not have a SAAR form available. <p>However, DFAS Centers periodically reviewed user access roles for appropriateness, but did not determine whether these 12 HQSA users were appropriate.</p> <p>Although DFAS Centers periodically reviewed user access roles for appropriateness, some of the DFAS Centers had a questionable number of users assigned the HQSA role. Specifically:</p> <ul style="list-style-type: none"> - DFAS-Arlington had 13 users assigned the HQSA role. - DFAS-Denver had 10 users assigned the HQSA role. - DFAS-Columbus had 17 users assigned the HQSA role. <p><u>DFAS-Arlington</u> The DDRS-AFS SAAR form used prior to 2004 did not include specific role categories for which a user had been authorized.</p> <p><u>DFAS-Cleveland</u> The import sheets uploaded into</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				<p>DDRS-AFS did not require approval prior to posting.</p> <p>The trial uploads and balance adjustments entered into DDRS-AFS do not require approval prior to posting.</p> <p><u>DFAS-Denver</u> A systems developer in Cleveland was assigned access to the production environment as a HQSA, which creates segregation of duties risks.</p>
		<p>5. DDRS-AFS application controls ensure that direct trial balance entries into DDRS-AFS and edits to the trial balance are in balance prior to updating the reporting tables.</p>	<p>Observed trial balance entry to determine whether control totals over data entered directly into DDRS-AFS ensured the trial balance was in balance prior to updating DDRS.</p> <p>Randomly sampled Microsoft Excel trial balances at 2004 FYE and Q1 2005 to determine whether direct trial balance entries into DDRS-AFS, and edits to the trial balance, were complete and in balance prior to updating the DDRS-AFS reporting tables.</p> <p>Confirmed, through corroborative inquiry, that direct trial balance entries into DDRS-AFS, and edits to the trial</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			balance, were complete and in balance prior to updating the DDRS-AFS reporting tables.	
		6. The entry and approval functions pertaining to the direct entering of trial balances or editing of trial balances are properly segregated between the individual entering the data and the individual approving the data.	<p>Inspected a list of DDRS-AFS users assigned the Data Administrator role, and the HQSA role, to determine whether this access was appropriate for their job responsibilities. HQSA is a powerful role that, while necessary on a limited basis, does not encompass the principles of separation of duties and least privileges.</p> <p>Obtained a random sample of trial balance upload system audit trails to determine whether trial balance uploads contain an approval.</p> <p>Confirmed, through corroborative inquiry, that direct trial balance entries into DDRS-AFS or edits to the trial balance were approved by an individual other than who entered the balance prior to updating the DDRS-AFS reporting tables.</p>	<p><u>DFAS-Arlington</u> <u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>Users were assigned roles based on each DFAS center's reporting activities which may provide them with access to multiple entity codes that they may not necessarily need. Also, trial balance corrections or adjustments, which can only be made by re-importing the trial balance, did not require approval.</p>
		7. DDRS-AFS maintains a closing date for the trial balance entry function to ensure Journal Voucher or trial balance adjustments are not made to the trial balance subsequent to external reporting.	Inspected the system audit log indicating the lockout occurred and observed that the lockout mechanism was enabled prior to the release of the statements to OMB, and that the mechanism	<u>DFAS-Arlington</u> No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>was effective in preventing additional adjustments to the financial statements.</p> <p>Confirmed, through corroborative inquiry, that a closing date maintained for the trial balance entry function ensures that Journal Vouchers or trial balance adjustments are not made to the trial balance subsequent to external reporting.</p>	
		<p>8. Controls ensure that the trial balance entered into DDRS-AFS is based on the current reporting period.</p>	<p>Inspected the trial balance import sheet to determine if data checks were enabled to allow DDRS-AFS to confirm that the period for which trial balance information was being imported was the current reporting period.</p> <p>Confirmed, through corroborative inquiry, that the trial balance entered into DDRS-AFS was based on the intended reporting period.</p>	<p><u>DFAS-Cleveland</u> Information contained on the Microsoft Excel trial balance import sheets did not indicate the quarterly reporting period that the uploaded information pertained to. However, as a mitigating control, the local unique process to prepare balances for import into DDRS-AFS contained controls to ensure that the balances are being imported for the current reporting period. Additionally, as a mitigating control, reconciliations would detect an incorrect upload that was not related to the current period. Thus, the control activity and the associated mitigating control supported the control objective.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>9. Trial balance and adjustment numbers for the reporting period are sent to the reporting activity for review of appropriateness and authorization.</p>	<p>Randomly sampled Microsoft Excel trial balances at 2004 FYE and at Q1 2005 to determine whether trial balance and adjustment numbers for the reporting period were sent to the reporting activity for review of appropriateness and authorization.</p> <p>Confirmed, through corroborative inquiry, that trial balance and adjustment numbers for the reporting period were sent to the reporting activity for review of appropriateness and authorization.</p>	<p><u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>No relevant exceptions noted.</p>
		<p>10. Significant policies and procedures are documented.</p>	<p>Inspected policies and procedures to determine whether significant policies and procedures were documented.</p> <p>Confirmed, through corroborative inquiry, that significant policies and procedures were documented.</p>	<p><u>DFAS-Cleveland</u></p> <p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
7	<i>USSGL Account Maintenance</i>			
	<p>Controls provide reasonable assurance that only valid and accurate changes are made to the DDRS-AFS Reference Tables, Department Reporting Tables and other critical system components; these changes are input and processed timely.</p> <p>Controls provide reasonable assurance that new accounting line items are promptly added to the reference tables and obsolete accounts are promptly removed, and only valid accounts are added to the reference table.</p>	<p>1. Reporting and account reference tables are periodically reviewed for accuracy and ongoing pertinence.</p>	<p>Inspected the DDRS-AFS USSGL change request log and DDRS-AFS USSGL system change log to determine whether tables were periodically reviewed for accuracy and ongoing pertinence.</p> <p>Confirmed, through corroborative inquiry, that reporting and account reference tables were periodically reviewed for accuracy and ongoing pertinence.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>
		<p>2. Requests to change the reporting and account reference table data in DDRS-AFS are documented in a USSGL change log and the log is reviewed to ensure that all requested changes are processed timely.</p>	<p>Inspected change requests to determine whether requests to change the reporting and account reference table data were logged; also, inspected USSGL change log to determine timeliness of changes.</p> <p>Confirmed, through corroborative inquiry, that requests to change the reporting and account reference table data were logged; the log was reviewed to ensure that all requested changes were processed timely.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>3. Changes to DDRS-AFS reporting and account reference tables are compared to the authorized USSGL change request originated by DFAS-Arlington accounting to ensure that they were input accurately by the DFAS-Arlington PMO.</p>	<p>Inspected change requests to determine whether changes to the reporting and account reference tables were compared to authorized USSGL change requests to ensure that they were input accurately.</p> <p>Confirmed, through corroborative inquiry, that changes to the reporting and account reference tables were compared to authorized USSGL change requests to ensure that they were input accurately.</p>	<p><u>DFAS-Arlington</u> <u>DFAS-Cleveland</u></p> <p>Changes documented in the USSGL change log were not reviewed and approved to determine if they were accurately entered. Also, changes were found to occasionally be made during production hours. However, some compensating controls existed. For instance, errors in the report mapping were identified and investigated as a part of the reporting process. Additionally, periodic USSGL reviews were performed to determine if they were consistent with the U.S. Treasury USSGL.</p>
		<p>4. The ability to view, modify, or transfer information contained in DDRS-AFS reporting and account reference tables is restricted to authorized personnel.</p>	<p>Selected a random sample of DFAS-AFS users to determine if SAAR forms matched the access provided.</p> <p>Inspected a list of DDRS-AFS users assigned the CFO_Table_Maint role, and the HQSA role, to determine whether this access was appropriate for their job responsibilities. HQSA is a powerful role that, while necessary on a limited basis, does not encompass the principles of separation of duties and least privileges.</p>	<p>Out of 162 total SAAR forms tested for all DDRS-AFS users, eight related to users of the DDRS_CFO_TABLE_MAINTAINANCE role which provides users with this role the ability to make changes to the US_SGL account structure in DDRS-AFS. Of these eight users:</p> <ul style="list-style-type: none"> - Four users had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or DFAS center to which access should be granted; and, - One user had a post 2004 SAAR form on file, but the DDRS-AFS role granted on the form did not

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>Confirmed, through corroborative inquiry, that the ability to view, modify, or transfer information contained in the reporting and account reference tables was restricted to authorized personnel.</p>	<p>match access provided in DDRS-AFS.</p> <p>However, DFAS Centers periodically reviewed user access roles for appropriateness</p> <p>Out of 162 total SAAR forms tested for all DDRS-AFS users, 12 related to users of the DDRS_CFO_HQSA role which provides users with this role the ability to assign and remove roles in DDRS-AFS. Of these 12 users:</p> <ul style="list-style-type: none"> - Nine users had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or DFAS center to which access should be granted; - Two users had a post 2004 SAAR form on file, but the DDRS-AFS role granted on the form did not match access provided in DDRS-AFS; and, - One user did not have a SAAR form available. <p>However, DFAS Centers periodically reviewed user access roles for appropriateness, but did not determine whether these 12 HQSA users were appropriate.</p> <p>Although DFAS Centers periodically reviewed user access roles for appropriateness, some of the DFAS Centers had a</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				<p>questionable number of users assigned the HQSA role. Specifically:</p> <ul style="list-style-type: none"> - DFAS-Arlington had 13 users assigned the HQSA role. - DFAS-Denver had 10 users assigned the HQSA role. - DFAS-Columbus had 17 users assigned the HQSA role. <p><u>DFAS-Arlington</u> The DDRS-AFS SAAR form used prior to 2004 did not include specific role categories for which a user had been authorized.</p> <p>Of 17 users assigned the CFO_Table_Maint role, 13 were identified that should not have been granted that role, although these users were subsequently removed based on the internal user review process.</p> <p><u>DFAS-Denver</u> A systems developer in Cleveland was assigned access to the production environment as a HQSA, which creates segregation of duties risks.</p>
		5. The functionality pertaining to the DDRS-AFS reporting and account reference tables allow the PMO to enter, edit, and store table changes so that the changes automatically become effective.	Inspected the USSGL account maintenance reference tables to determine whether the functionality pertaining to the reporting and account reference tables allowed the user to enter,	<u>DFAS-Arlington</u> No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			<p>edit, and store accounting classification table changes so that the changes automatically became effective.</p> <p>Confirmed, through corroborative inquiry, that the reporting and account reference tables allowed the user to enter, edit, and store accounting classification table changes so that the changes automatically became effective.</p>	
		<p>6. DDRS-AFS will reject or suspend interfaced USSGL accounts that contain accounting classification elements or domain values that have been deactivated or discontinued.</p>	<p>Observed DDRS-AFS edit checks to determine whether the reporting and account reference tables allowed the system to reject or suspend interfaced transactions that contained accounting classification elements or domain values that had been deactivated or discontinued.</p> <p>Confirmed, through corroborative inquiry, that DDRS-AFS will reject or suspend interfaced transactions that contain accounting classification elements or domain values that have been deactivated or discontinued.</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
8	<i>USSGL & Other Guidelines</i>			
	<p>Controls provide reasonable assurance that DDRS-AFS produces financial statements that conform to the USSGL.</p> <p>Controls provide reasonable assurance that any relevant changes made to the USSGL by the Treasury Department are included in the reference tables, and that changes to the tables are authorized and approved.</p>	<p>1. DDRS-AFS financial statements are consistent with the USSGL as published by the U.S. Treasury.</p>	<p>Compared DDRS-AFS module chart of accounts with the USSGL to determine whether it was consistent with the USSGL.</p> <p>Inspected the DDRS-AFS report maps to determine whether the financial statements are consistent with the USSGL.</p>	<p><u>DFAS-Arlington</u> DoD policies related to the preparation of financial statements and the template used for preparation of financial statements did not provide for reporting a significant amount of accounting information required by the Federal Accounting Standards Advisory Board (FASAB) and Office of Management and Budget (OMB) Bulletin 01-09. Also, the mapping of accounts for the preparation of financial statements in several instances relied upon DoD general ledger accounts, instead of USSGL account codes. Furthermore, the mapping of accounts used for the preparation of the Statement of Custodial Activity did not conform to Treasury requirements.</p>
		<p>2. Data converted from the Report on Budget Execution and Budgetary Resources (SF-133) and entered into DDRS-AFS is consistent with the Statement of Budgetary Resources.</p>	<p>Inspected the reconciliation reports that DFAS-Arlington required from DFAS centers for FY 04 and FY 05 Q1 to determine whether the reconciliation between Statement of Budgetary Resources and Report on Budget Execution and Budgetary Resources (SF-133.) was performed and differences explained.</p>	<p><u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>Although the SF-133 and Statement of Budgetary Resources reconciliation was performed, management did not sign off on the series of reconciliation reports evidencing a review before the reconciliation was submitted to DFAS-Arlington.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			Confirmed, through corroborative inquiry, that data converted from the Report on Budget Execution and Budgetary Resources (SF-133) entered into DDRS-AFS was consistent with the Statement of Budgetary Resources.	
		3. Prior to each reporting period or on a periodic basis, the USSGL is reviewed for changes applicable to the DDRS-AFS module chart of accounts to ensure accuracy and pertinence.	<p>Compared DDRS-AFS module chart of accounts to updates in the Quarterly Guidance to determine if, prior to each reporting period or on a periodic basis, the USSGL was reviewed for changes applicable to the DDRS-AFS module chart of accounts.</p> <p>Confirmed, through corroborative inquiry, that prior to each reporting period or on a periodic basis, the USSGL was reviewed for changes applicable to the DDRS-AFS module chart of accounts to ensure accuracy and pertinence.</p>	<u>DFAS-Arlington</u> No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>4. Changes to the chart of accounts in the DDRS-AFS module are authorized and approved.</p>	<p>Obtained the DDRS-AFS offline change log maintained by DFAS-Arlington PMO to determine whether changes were authorized and approved.</p> <p>Confirmed, through corroborative inquiry, that changes to the chart of accounts in the DDRS-AFS module were authorized, approved, and tested prior to implementation.</p>	<p><u>DFAS-Arlington</u> Although changes to the chart of account were documented in the off-line change log, there was no documented process in place for reviewing or authorizing the change.</p>
		<p>5. Significant policies and procedures are documented.</p>	<p>Inspected significant policies and procedures to determine whether significant policies and procedures were documented.</p> <p>Confirmed, through corroborative inquiry, that significant policies and procedures were documented.</p>	<p><u>DFAS-Arlington</u> Procedures to make changes in DDRS-AFS related to the USSGL Chart of Accounts and mappings were not formally documented. A mitigating control existed because DDRS-AFS user manuals were available and changes in reporting requirement were disseminated to the DFAS-Arlington PMO. Thus, the control activity and associated mitigating control supported the control objective.</p>

Data Collection Module

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
1	<i>Audit Trails</i>			
	<p>Controls provide reasonable assurance that DDRS-DCM produces financial statements that are supported by audit trails that are adequate for the financial management entity and external auditors to trace amounts reported in the financial statement back to trial balances and data from feeder systems.</p> <p>Controls provide reasonable assurance that audit trails indicate the user inputting the trial balance and the user approving the trial balance. All audit trails indicate the user inputting the Journal Voucher and the user approving the Journal Voucher. Audit trails are reviewed on a regular basis for appropriateness.</p>	<p>1. Financial statement line item amounts in DDRS-AFS are drilled down to the detailed balance and activity supporting the line item numbers, including amounts entered manually into the DDRS-AFS module from DCM.</p>	<p>Selected a Journal Voucher from category M and noted the USSGL account posted. Performed a drill down on the corresponding Financial Statement line item containing the account until the Journal Voucher was displayed. Noted that the data in the Journal Voucher matched data in the Journal Voucher log.</p>	<p><u>DFAS-Indianapolis</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>2. Balances manually entered into DDRS-DCM are supported by audit trails that indicate the person, status, date input, and type (e.g., consolidating).</p>	<p>Scanned the audit trail and determined that transactions were captured in DDRS-DCM and that they included the User ID, date of transaction, and amount of transaction.</p> <p>Confirmed, through corroborative inquiry, that balances manually entered into DDRS-DCM, balances imported via Microsoft Excel import sheets and balances imported from DDRS-DCM entry were supported by audit trails that indicated the user ID inputting the trial balance, the date and time input, and an indicator of how the balance has been entered online.</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p>
		<p>3. Balances entered into DDRS-DCM are supported by audit trails indicating the User ID, date the balance was entered, and the User ID approving the balance.</p>	<p>Scanned the audit trail and determined if transactions were captured in DDRS-DCM and that they included the User ID and date the balance was entered, and the User ID approving the balance.</p> <p>Confirmed, through corroborative inquiry, that balances entered into DDRS-DCM were supported by audit trails indicating the User ID and date the balance was entered and the User ID approving the balance.</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		4. During each accounting quarter or other reporting period, audit trails in the DDRS-DCM are periodically reviewed for appropriateness and unusual activity.	Confirmed, through corroborative inquiry, that during each accounting quarter or other reporting period, audit trails in the DDRS-DCM were periodically reviewed for appropriateness and unusual activity.	<u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> Audit logs were not reviewed.
		5. All cancelled Journal Vouchers keyed into DDRS-AFS from DDRS-DCM contained a Journal Voucher ID number and the dates and times they were cancelled or rejected.	Reviewed system log in DDRS-AFS to determine if cancelled Journal Vouchers contained a Journal Voucher ID number and dates and times they were cancelled or rejected. Confirmed, through corroborative inquiry, that all cancelled Journal Vouchers keyed into DDRS-AFS from DDRS-DCM contained a Journal Voucher ID number and the dates and times they were cancelled or rejected.	<u>DFAS-Cleveland</u> In DDRS-AFS, cancelled Journal Vouchers were recorded; however, Journal Voucher cancellations were not displayed in the Journal Voucher log with the canceling user's ID, date cancelled, or reason cancelled. Cancelled Journal Vouchers did not affect the financial statements.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
2	Balance Entry			
	<p>Controls provide reasonable assurance that balances entered into the DDRS-DCM are supported by adequate documentation, and that balances entered into the DDRS-DCM are approved prior to entry into a DDRS table.</p> <p>Controls provide reasonable assurance that the separation of duties exists to ensure the person approving the balances entered into the DDRS-DCM is not the person entering the balances entered into the DDRS-DCM.</p> <p>Controls provide reasonable assurance that balances entered into the DDRS-DCM are in balance prior to entry into DDRS-AFS.</p>	<p>1. Data call information imported from DDRS-DCM into DDRS-AFS as Journal Vouchers are supported by adequate documentation.</p>	<p>Reviewed entry from DCM to DDRS-AFS and determined that entries were supported by adequate documentation and approved prior to entry into the DDRS-DCM.</p> <p>Confirmed, through corroborative inquiry, that data call information imported from DDRS-DCM into DDRS-AFS as Journal Vouchers was supported by adequate documentation.</p>	<p><u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u></p> <p>No relevant exceptions noted.</p>
		<p>2. The ability to enter or modify information contained in a balance is restricted to authorized personnel.</p>	<p>Confirmed users with ability to enter or approve balances by obtaining the SAAR form and confirming that the user is allowed to enter balances.</p> <p>Used the Financial Audit Manual guide on population size to judgmentally select a sample of 80 SAAR forms for testing.</p> <p>Confirmed, through corroborative inquiry, that the ability to enter or modify information contained in a balance was restricted to</p>	<p><u>DFAS-Arlington</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u></p> <p>Out of 80 total SAAR forms tested for all DDRS-DCM users, 32 related to users of the Data Entry role which provide users with this role the ability to enter and finalize balances entered into DDRS-DCM. Of these 32 users: - 23 users had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or reporting area in DDRS-DCM to which</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			authorized personnel.	access should be granted; - Two users had a post 2004 SAAR form on file, but the specific role was not indicated on the form; and, - One users access granted in DDRS-DCM did not match the access provided in the form.
		3. The balances entered are approved or rejected by an individual other than who entered the balance and who has authority to approve or reject the balance.	<p>Confirmed users with ability to enter or approve balances by obtaining the SAAR form and confirming that the user is allowed to enter balances.</p> <p>Reviewed DCM balance entry in DDRS-AFS and determined that balances must be approved. Determined that Journal Vouchers during DDRS-AFS import must be approved.</p> <p>Confirmed, through corroborative inquiry, that the balances entered were approved or rejected by an individual other than who entered the balance and who had authority to approve or reject the balance.</p>	<p><u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u></p> <p>Out of 80 total SAAR forms tested for all DDRS-DCM users, 27 related to users of the Consolidator role which provide users with this role the ability to consolidate and approve balances entered into DDRS-DCM. Of these 27users; - Eighteen users had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or reporting area in DDRS-DCM to which access should be granted; and, - One user had a post 2004 SAAR form on file, but the specific role was not indicated on the form.</p> <p>However, DFAS Centers periodically reviewed user access roles for appropriateness. Consolidators can approve their own balance entries in DCM; however, the Journal Vouchers put into DDRS-AFS must be approved by someone other than the Journal Voucher creator.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>4. The data call information in the DDRS-DCM is in balance before being imported as a Journal Voucher into DDRS. Within DDRS-DCM, data calls entered out-of-balance will be prompted with an error message and not recorded until balanced.</p>	<p>Inspected process for establishing Journal Vouchers in DDRS-AFS from DDRS-DCM and confirmed that each cell in DDRS-DCM contains a Journal Voucher which must be in balance prior to updating DDRS-AFS.</p> <p>Confirmed, through corroborative inquiry, that data call information in the DDRS-DCM was in balance before being imported as a Journal Voucher into DDRS. Within the DDRS-DCM data calls entered out-of-balance were prompted with an error message and not recorded until balanced.</p>	<p><u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u></p> <p>No relevant exceptions noted.</p>
		<p>5. Data calls in DDRS-DCM creating the Journal Vouchers to be imported into DDRS-AFS are included in the intended reporting period.</p>	<p>Inspected Journal Voucher input process in DDRS-AFS and noted that Journal Vouchers could only be input for the current period.</p> <p>Confirmed, through corroborative inquiry, that the data calls in DDRS-DCM creating the Journal Vouchers to be imported into DDRS were included in the intended reporting period.</p>	<p><u>DFAS-Indianapolis</u></p> <p>No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>6. The balances keyed in from DDRS-DCM to DDRS-AFS as Journal Vouchers update all applicable general ledger account balances (i.e., budgetary, proprietary and memorandum accounts) based on a single input transaction and are included in the final trial balance numbers.</p>	<p>Selected random sample of Journal Vouchers in DDRS-AFS and determined that they update all applicable general ledger account balances (i.e., budgetary, proprietary and memorandum accounts) based on a single input transaction and were included in the final trial balance numbers.</p> <p>Confirmed, through corroborative inquiry, that the balances keyed in from DDRS-DCM to DDRS-AFS as Journal Vouchers updated all applicable general ledger account balances (i.e., budgetary, proprietary and memorandum accounts) based on a single input transaction and were included in the final trial balance numbers.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>
		<p>7. A closing date on Journal Vouchers imported into DDRS-AFS from DDRS-DCM enables DFAS personnel to ensure no Journal Voucher adjustments are made to the trial balance subsequent to external reporting.</p>	<p>Inspected the system audit log in DDRS-AFS indicating the lockout occurred and confirmed that the lockout mechanism was enabled prior to the release of the statements to OMB, and that the mechanism was effective in preventing additional adjustments to the financial statements.</p> <p>Confirmed, through corroborative inquiry, that a closing date on Journal Vouchers imported into DDRS-</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
			AFS from DDRS-DCM enabled DFAS personnel to ensure no Journal Voucher adjustments were made to the trial balance subsequent to external reporting.	
		8. Journal vouchers imported or keyed into DDRS-AFS from DDRS-DCM are assigned Journal Voucher control numbers prior to approval and, after approval, are given sequential approved Journal Voucher ID numbers; the numerical sequence of each Journal Voucher is accounted for to ensure that all Journal Vouchers are processed timely.	<p>Inspected the Journal Voucher log in DDRS-AFS to determine whether it was sequentially ordered, and, if breaks in the sequence of control numbers existed, whether they were explained.</p> <p>Confirmed, through corroborative inquiry, Journal Vouchers imported or keyed into DDRS-AFS from DDRS-DCM were assigned Journal Voucher control numbers prior to approval and, after approval, were given sequential approved Journal Voucher ID numbers; the numerical sequence of each Journal Voucher was accounted for to ensure that all Journal Vouchers are processed timely.</p>	<u>DFAS-Cleveland</u> Inspection of the Journal Voucher log showed that some numbers were missing from the sequence of Journal Vouchers numbers as a result of a trial balance and associated Journal Vouchers being deleted.
		9. Journal vouchers for the reporting period are available to the reporting activity for review of appropriateness and authorization.	Confirmed, through corroborative inquiry, that reports of Journal Vouchers for the reporting period were sent to the reporting activity for review of appropriateness and authorization.	<u>DFAS-Cleveland</u> No relevant exceptions noted.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
3	<i>Validation</i>			
	<p>Controls provide reasonable assurance that the DDRS-DCM has systems or processes for determining the quality and integrity of data flowing through the system, and trial balances are input and updated completely and accurately.</p> <p>Controls provide reasonable assurance that data validation and editing are performed to identify erroneous data, and that erroneous data are captured, reported, investigated, and corrected.</p>	<p>1. Control totals over data entered directly into the DDRS-DCM ensure the journal entries are in balance prior to updating DDRS-AFS and are being updated to the correct entity.</p>	<p>Inspected process for establishing Journal Vouchers in DDRS-AFS from DDRS-DCM and confirmed that each cell in DDRS-DCM contains a Journal Voucher which must be in balance prior to updating DDRS-AFS.</p> <p>Confirmed, through corroborative inquiry, that control totals over data entered directly into the DDRS-DCM ensured the trial balance or journal entry was in balance prior to updating DDRS.</p>	<p><u>DFAS-Cleveland</u> No relevant exceptions noted.</p>
		<p>2. Transactions are automatically assigned a unique sequence number. (Only in a Journal Voucher output process.)</p>	<p>Inspected the Journal Voucher log in DDRS-AFS to determine whether it was sequentially ordered, and, if breaks in the sequence of control numbers existed, whether they were explained.</p> <p>Confirmed, through corroborative inquiry, that transactions were automatically assigned a unique sequence number. (Only in a Journal Voucher output process.)</p>	<p><u>DFAS-Cleveland</u> Inspection of the Journal Voucher log showed that some numbers were missing from the sequence of Journal Vouchers numbers as a result of a trial balance and associated Journal Vouchers being deleted.</p>

Data Collection Module Interfacing

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
1	Validation			
	Controls provide reasonable assurance that DDRS has systems or processes for determining the quality and integrity of data flowing through the system, and balances are input and updated completely and accurately.	1. Controls over data entered directly into DDRS-AFS from DDRS-DCM of DDRS ensure the journal entry is in balance prior to updating DDRS-AFS.	<p>Inspected process for establishing Journal Vouchers in DDRS-AFS from DDRS-DCM and confirmed that each cell in DDRS-DCM contains a Journal Voucher which must be in balance prior to updating DDRS-AFS.</p> <p>Confirmed, through corroborative inquiry, that controls over data entered directly into the AFS Module from DDRS-DCM ensured the trial balance or journal entry was in balance prior to updating DDRS-DCM.</p>	<p><u>DFAS-Indianapolis</u> <u>DFAS-Cleveland</u></p> <p>No relevant exceptions noted.</p>
		2. The data imported or keyed from DCM creates complete Journal Vouchers adjustments pending approval by DFAS staff.	<p>Inspected DDRS-DCM entries in DDRS-AFS and confirmed the entries are approved.</p> <p>Inspected audit logs in DDRS-AFS and determined that Journal Vouchers had been approved.</p> <p>Confirmed, through corroborative inquiry, that the data imported or keyed in from DCM created complete Journal Vouchers adjustments pending approval by DFAS staff.</p>	<p><u>DFAS-Arlington</u> <u>DFAS-Columbus</u> <u>DFAS-Indianapolis</u></p> <p>Although the Journal Vouchers keyed into DDRS-AFS must be approved, users are frequently re-keying data from DCM into AFS, which can circumvent the systemic approval controls for DCM. At DFAS-Indianapolis, balances manually keyed into DDRS-AFS were not always approved.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
2	<i>Authorized Entry</i>			
	<p>Controls provide reasonable assurance that data transmissions between DDRS-AFS and DDRS DCM are authorized, complete, accurate and secure. Unbalanced trial balances are flagged and not reported until in balance.</p>	<p>1. Transmissions to DDRS-AFS were initiated automatically or by authorized personnel.</p>	<p>Selected a random sample of DFAS-AFS users to determine if SAAR forms matched the access provided.</p> <p>Inspected a list of DDRS-AFS users assigned the data administrator role, which allows initiation of a transmission to DDRS-AFS, and the HQSA role, to determine whether this access was appropriate for their job responsibilities. HQSA is a powerful role that, while necessary on a limited basis, does not encompass the principles of separation of duties and least privileges. Inspected e-mail traffic to confirm that DFAS Centers periodically review user access for appropriateness.</p> <p>Confirmed, through corroborative inquiry, that trial balance transmissions to DDRS-AFS were initiated automatically or by authorized personnel.</p>	<p>Controls were designed to provide for access to DDRS-AFS on a center-level basis, instead of by responsible work area. As such, the user may have access to information that they don't necessarily need.</p> <p>Out of 162 total SAAR forms tested for all DDRS-AFS users, five related to users of the DDRS_CFO_DATA_ADMIN role which provides users with this role the ability to import DCM balances into DDRS-AFS. Of these five users:</p> <ul style="list-style-type: none"> - One user had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or DFAS center to which access should be granted. - Two users had a post 2004 SAAR form on file, but the DDRS-AFS role granted on the form did not match access provided in DDRS-AFS. <p>However, DFAS Centers periodically reviewed user access roles for appropriateness.</p> <p>Out of 162 total SAAR forms tested for all DDRS-AFS users, 12 related to users of the DDRS_CFO_HQSA role which</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				<p>provides users with this role the ability to assign and remove roles in DDRS-AFS. Of these 12 users:</p> <ul style="list-style-type: none"> - Nine users had a SAAR form on file dated prior to 2004, which did not provide enough detail to indicate the user role or DFAS center to which access should be granted. - Two users had a post 2004 SAAR form on file, but the DDRS-AFS role granted on the form did not match access provided in DDRS-AFS. - One user did not have a SAAR form available. <p>However, DFAS Centers periodically reviewed user access roles for appropriateness, but did not determine whether these 12 HQSA users were appropriate.</p> <p>Although DFAS Centers periodically reviewed user access roles for appropriateness, some of the DFAS Centers had a questionable number of users assigned the HQSA role. Specifically:</p> <ul style="list-style-type: none"> - DFAS-Arlington had 13 users assigned the HQSA role. - DFAS-Denver had 10 users assigned the HQSA role. - DFAS-Columbus had 17 users assigned the HQSA role.

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				<p><u>DFAS-Arlington</u> The DDRS-AFS SAAR form used prior to 2004 did not include specific role categories for which a user had been authorized.</p> <p><u>DFAS-Cleveland</u> The trial uploads and balance adjustments entered into DDRS-AFS do not require approval prior to posting.</p> <p><u>DFAS-Denver</u> A systems developer was assigned access to the production environment as a HQSA, which creates segregation of duties risks.</p>
3	<i>USSGL & Other Guidelines</i>			
	<p>Controls provide reasonable assurance that the DDRS-DCM assists DDRS-AFS to produce financial statements that conform to the USSGL. Controls provide reasonable assurance that any relevant changes made to the USSGL by the Treasury Department are included in the Reference Tables, and that changes to the tables are authorized and approved.</p>	<p>1. DDRS-AFS transmissions from DDRS-DCM are consistent with that of the USSGL as published by the U.S. Treasury.</p>	<p>Compared DDRS-AFS chart of accounts with the USSGL to determine whether it was consistent with the USSGL.</p> <p>Confirmed, through corroborative inquiry, that DDRS-AFS transmissions from DDRS-DCM were consistent with that of the USSGL as published by the U.S. Treasury department and that the USSGL account tables for DDRS-DCM and DDRS-AFS were the same.</p>	<p><u>DFAS-Arlington</u> DoD policies related to the preparation of financial statements and the template used for preparation of financial statements did not provide for reporting a significant amount of accounting information required by the Federal Accounting Standards Advisory Board (FASAB) and Office of Management and Budget (OMB) Bulletin 01-09. Also, the mapping of accounts for the preparation of financial statements in several instances relied upon DoD general ledger accounts, instead of USSGL account codes. Furthermore, the mapping of</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				accounts used for the preparation of the Statement of Custodial Activity did not conform to Treasury requirements.
		2. Prior to each reporting period or on a periodic basis, the USSGL is reviewed for changes applicable to the DDRS-AFS Module from the Data Collection Module chart of accounts to ensure accuracy and pertinence.	<p>Compared DDRS-AFS module chart of accounts to updates in the Quarterly Guidance to determine if, prior to each reporting period or on a periodic basis, the USSGL was reviewed for changes applicable to the DDRS-AFS module chart of accounts.</p> <p>Confirmed, through corroborative inquiry, prior to each reporting period or on a periodic basis, the USSGL is reviewed for changes applicable to the DDRS-AFS Module from the Data Collection Module chart of accounts to ensure accuracy and pertinence.</p>	<u>DFAS-Arlington</u> No relevant exceptions noted.
		3. Changes to the chart of accounts in DDRS-AFS Module from DDRS-DCM are authorized, approved, and tested prior to implementation.	<p>Obtained the DDRS-AFS offline change log maintained by DFAS-Arlington PMO to determine whether changes were authorized and approved.</p> <p>Confirmed, through corroborative inquiry, that changes to the chart of accounts in the DDRS-AFS Module from the Data Collection Module were authorized, approved, and tested prior to implementation.</p>	<u>DFAS-Arlington</u> Although changes to the chart of account were documented in the off-line change log, there was not a documented process in place for reviewing and authorizing the change.

Local Unique Processes

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
1	<i>Local Unique Process</i>			
	<p>Controls provide reasonable assurance that trial balance data manually migrated into DDRS-AFS is accurate, authorized, and complete. Data from the Report on Budget Execution and Budgetary Resources (SF-133) or feeder systems are input accurately into DDRS-AFS. Any reclassifications are authorized and approved and are monitored by an audit trail.</p>	<p>1. Output reports from reporting activities feeder systems are from authorized personnel or source.</p>	<p>Scanned output reports and evidence the output reports were received from authorized personnel or source.</p> <p>Confirmed, through corroborative inquiry, that output reports from reporting activities feeder systems are from authorized personnel or source.</p>	<p><u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>No relevant exceptions noted.</p>
		<p>2. Output reports from reporting activities feeder systems are complete and in balance.</p>	<p>Scanned output reports and evidence they were complete and in balance.</p> <p>Confirmed, through corroborative inquiry, that output reports from reporting activities feeder systems were complete and in balance.</p>	<p><u>DFAS-Cleveland</u> <u>DFAS-Columbus</u></p> <p>Proprietary balances are derived from budgetary accounts.</p> <p>Reconciling items remain unresolved in the DDRS-AFS local unique process.</p> <p><u>DFAS-Columbus</u> Performed estimated allocations of Trading Partner data.</p> <p><u>DFAS-Denver</u> Budgetary balances are derived from proprietary accounts. Additionally, a modified version of the import sheet is used at DFAS-Denver which does not contain all the built in controls. However, the sheet does have a balancing</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
				formula and DDRS-AFS import verification controls apply.
		3. Local unique processes to prepare the data for DDRS-AFS import are reviewed and approved.	<p>Scanned output reports to determine if the local unique processes to prepare the data for DDRS-AFS import was reviewed and approved.</p> <p>Confirmed, through corroborative inquiry, that the local unique processes to prepare the data for DDRS-AFS import were reviewed and approved.</p>	<p><u>DFAS-Cleveland</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u></p> <p>Reviews and approvals did not occur and there was no separation of duties in the uploading of balances. However, the customer confirmed the balances in DDRS.</p> <p><u>DFAS-Indianapolis</u> Uploads of the trial balance import sheet were not required to be approved.</p>
		4. Adjustments made during the local unique processes to prepare the data for DDRS-AFS import are reviewed and approved.	<p>Inspected local unique process to prepare the data for DDRS-AFS import and evidence that trial balance adjustments were reviewed and approved.</p> <p>Confirmed, through corroborative inquiry, that adjustments made during the local unique processes to prepare the data for DDRS-AFS import were reviewed and approved.</p>	<p><u>DFAS-Cleveland</u> Fiscal year end 2004 adjustments to trial balances were not approved. At first quarter 2005, the trial balances adjustments were approved in DDRS-AFS.</p> <p><u>DFAS-Denver</u> A single FICA equity adjustment was made offline and was not reviewed and approved.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		<p>5. Adjustments made during the local unique processes to prepare the data for DDRS-AFS import are supported by an audit trail.</p>	<p>Scanned the Microsoft Excel worksheets to determine if adjustments made during the local unique processes to prepare the data for DDRS-AFS import were supported by an audit trail.</p> <p>Confirmed, through corroborative inquiry, that adjustments made during the local unique processes to prepare the data for DDRS-AFS import were supported by an audit trail.</p>	<p><u>DFAS-Cleveland</u> Trial balance adjustments at quarter four 2004 were not supported by an audit trail.</p> <p><u>DFAS-Denver</u> Single FICA equity adjustment was made offline and was not supported by an audit trail.</p>
		<p>6. A closing date on reporting enables DFAS personnel to ensure no Journal Voucher or trial balance adjustments are made to the trial balance subsequent to external reporting.</p>	<p>Inspected the DDRS-AFS system audit log indicating the lockout occurred and observed that the lockout mechanism was enabled prior to the release of the statements to OMB, and that the mechanism was effective in preventing additional adjustments to the financial statements.</p> <p>Confirmed, through corroborative inquiry, that a closing date on reporting enabled DFAS personnel to ensure no Journal Voucher or trial balance adjustments were made to the trial balance subsequent to external reporting.</p>	<p><u>DFAS-Arlington</u> No relevant exceptions noted.</p>

CO No.	Control Objective	Control Activity	Test Procedure	Results of Testing
		7. Feeder system reports and trial balance uploads during the local unique processes to prepare the data for DDRS-AFS import are based on the intended reporting period.	Scanned output reports to determine if feeder system reports and trial balance uploads during the local unique processes to prepare the data for DDRS-AFS import were based on the proper reporting period. Confirmed, through corroborative inquiry, that feeder system reports and trial balance uploads during the local unique processes to prepare the data for DDRS-AFS import were based on the proper reporting period.	<u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u> No relevant exceptions noted.
		8. Final balance numbers are confirmed by the customer.	Inspected the contents of the Confirmation Letter issued by the customer to signify the review and acceptance of the financial statements prepared by DFAS.	<u>DFAS-Cleveland</u> <u>DFAS-Indianapolis</u> <u>DFAS-Columbus</u> <u>DFAS-Denver</u> No relevant exceptions noted.
		9. All critical procedures were documented.	Determined that all critical procedures were documented. Confirmed, through corroborative inquiry, all critical procedures were documented.	<u>DFAS-Cleveland</u> Local unique procedures for the standard reporting checklist were documented but not implemented. <u>DFAS-Columbus</u> Local unique data import process was not standardized. Some procedures were not clearly documented. <u>DFAS-Denver</u> Procedures were not documented.

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

IV. Supplemental Information Provided by the Defense Information Systems Agency

This information has not been subjected to the procedures applied to the examination of the description of controls presented in Sections II and III of this report, and accordingly, the DoD OIG expresses no opinion regarding the completeness and accuracy of this information.

To accommodate a major disaster at any major DISA processing center, DISA has established the DISA Continuity and Test Facility (DCTF) at Slidell, LA. This facility is equipped with computational, DASD (Direct Access Storage Device), and telecommunications resources sized to provide a fully functional host site with the capacity to support a major disaster at any DISA processing center.

The Continuity of Operations support agreement between DDRS, which is part of the DFAS Corporate Information Infrastructure (DCII), as the customer and DISA and as the provider of processing system and communications services, provides for restoring host site processing in the event of a major disaster and the timely resolution of problems during other disruptions that adversely affect DDRS processing.

The enterprise backup process is managed by DISA DECC-Ogden. Backup tapes containing the incremental daily and the complete weekly backups are created at Ogden. The tapes are rotated off site to Iron Mountain near Salt Lake City, UT for storage on a predetermined schedule.

The Crisis Management Team (CMT) at DISA DECC-Ogden is responsible for declaring that a disaster has occurred and initiating the Business Continuity Plan (BCP). The CMT will then activate the following response teams: Communications Team (COMT), Recovery Coordination Team (RCT), Site Recovery Team (SRT), and the Crisis Support Team (CST). Each team has a specific set of responsibilities defined in the Business Continuity Plan. The contact information for each individual on each team is also included in the Business Continuity Plan. The BCP is required to be evaluated on an annual basis.

The DDRS Continuity of Operations Plan (COOP) provides guidance on the DDRS software restoration for emergencies, disasters, mobilization, and for maintaining a state of readiness to provide the necessary level of information processing support commensurate with the mission requirements and priorities identified by the functional proponent. The DDRS COOP was written to serve as a bridge between the customers' site-unique COOPs and the DECC Ogden BCP. An annual review of the DDRS COOP will be performed. A test of the COOP is conducted every three years and consists of declaring one complete system platform inoperable at a given site.

Acronyms and Abbreviations

AIS	Automated Information System
AMO	Acquisition Management Organization
BCP	Business Continuity Plan
CAC	Common Access Card
CDOIM	Centralized Directorate for Information Management
CMIS	Configuration Management Information System
COOP	Continuity of Operations
DBA	Database Administrator
DCM	Data Collection Module
DDRS	Defense Departmental Reporting System
DECC	Defense Enterprise Computing Center
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DMZ	Demilitarized Zone
DoD	Department of Defense
DoD OIG	Department of Defense Office of Inspector General
DOIM	Defense Office of Information Management
FACTS	Federal Agencies Centralized Trial Balance System
FASAB	Federal Accounting Standards Advisory Board
FFMIA	Federal Financial Management Improvement Act
FMR	Financial Management Regulation
FRR	Functional Requirements Review
FSO	Field Security Operations
GCC	General Computer Control
GMRA	Government Management Reform Act
HQSA	Headquarters Security Administrator
IA	Information Assurance
IDS	Intrusion Detection System
OMB	Office of Management and Budget
PMO	Program Management Office
PVCS	Program Version Control System
SAAR	System Authorization Access Request
SAS	Statement on Auditing Standards
SLA	Service Level Agreement
SQA	Software Quality Assurance
SRR	Security Readiness Review
SSAA	System Security Authorization Agreement
STIG	Security Technical Implementation Guidelines
TSO	Technology Services Organization

USSGL
VPN

United States Standard General Ledger
Virtual Private Network

Report Distribution

Office of the Secretary of Defense

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

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

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

Combatant Command

Inspector General, U.S. Joint Forces Command

Other Defense Organizations

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

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
Government Accountability Office

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 Inspector General produced this report.

Paul J. Granetto
Patricia A. Marsh
Addie M. Beima
Michael Perkins
G. Marshall Grimes
Frank C. Sonsini
Ernest Fine
Chanda D. Lee
Laura Croniger
Richard M. Ng
Lauren S. McLean
Stanley J. Arceneaux
Mahalakshmi Krishnam
Randall D. Yoder
Emily M. Caldwell
Jose V. Morales-Santiago