

~~FOR OFFICIAL USE ONLY~~

Report No. D-2010-070

June 30, 2010

Inspector General

United States
Department of Defense



Defense Information Systems Agency Control Placed
in Operation and Tests of Operating Effectiveness for
the Period October 1, 2009 through April 30, 2010

~~Warning~~

~~"The enclosed document(s) is (are) the property of the Department of Defense, Office of Inspector General. Release or disclosure of the contents is prohibited by DOD Directive 5106.1. Contents may be disclosed only to persons whose official duties require access hereto. Contents cannot be released outside the Defense Department without the approval of the Department of Defense, Office of Inspector General."~~

~~FOR OFFICIAL USE ONLY~~

Additional Information and Copies

The Department of Defense Office of the Deputy Inspector General for Auditing, Defense Business Operations, prepared this report. If you have questions, contact the signer of the report.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (703) 604-8932, or by mail:

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

DEPARTMENT OF DEFENSE

hotline

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

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



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

June 30, 2010

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (COMPTROLLER)/
CHIEF FINANCIAL OFFICER
ASSISTANT SECRETARY OF DEFENSE (NETWORKS AND
INFORMATION INTEGRATION)/DOD CHIEF INFORMATION
OFFICER
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Defense Information Systems Agency Controls Placed in Operation and Tests of
Operating Effectiveness for the Period October 1, 2009 through April 30, 2010
(Report No. D-2010-070)

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

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 601-5868 (DSN 329-5868).

Patricia A. Marsh

Patricia A. Marsh, CPA
Assistant Inspector General
Defense Business Operations

~~FOR OFFICIAL USE ONLY~~

Table of Contents

Foreword	i
Section I	
Independent Service Auditor's Report	1
Section II	
Description of the Defense Information Systems Agency Operations and Controls Provided by the Defense Information Systems Agency	7
Section III	
Control Objectives, Control Activities, and Tests of Operating Effectiveness	25
Section IV	
Supplemental Information Provided by the Defense Information Systems Agency	49
Acronyms and Abbreviations	53

Foreword

This report is intended for the use of Defense Information Systems Agency (DISA) management, DISA customer organizations, and the independent auditors of its customer organizations. DOD personnel who manage the operating environments will also find this report of interest, as it contains information about DISA-operated general controls.

The DOD Office of Inspector General is implementing a long-range strategy to conduct audits of DOD financial statements. The Chief Financial Officers Act of 1990 (Public Law No. 101-576), as amended, mandates that agencies prepare and conduct audits of financial statements, which is key to achieving the goals of the Act.

This report focuses on the DISA Computing Services Directorate (CSD). CSD provides computer processing for the entire range of combat support functions, including transportation, logistics, maintenance, munitions, engineering, acquisition, finance, medicine, and military personnel readiness. CSD offers computing services on CSD and customer-owned platforms, including computer operations, data storage, systems administration, security management, capacity management, system engineering, Web and portal hosting, architectural development, and performance monitoring.

This examination assessed DISA-operated controls. Effective internal control is critical to achieving reliable information for all management reporting and decision-making. This report provides an opinion on the fairness of presentation, adequacy of design, and operating effectiveness of key controls that are relevant to audits of customer organization's financial statements. As a result, this examination precludes the need for customer organizations and their auditors to perform multiple audits of DISA in order to plan or conduct financial statement and performance audits.

Section I: Independent Service Auditor's Report

~~**FOR OFFICIAL USE ONLY**~~



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

June 30, 2010

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (COMPTROLLER)/
CHIEF FINANCIAL OFFICER
ASSISTANT SECRETARY OF DEFENSE (NETWORKS
AND INFORMATION INTEGRATION)/DOD CHIEF
INFORMATION OFFICER
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY

SUBJECT: Defense Information Systems Agency Controls Placed in Operation and
Tests of Operating Effectiveness for the Period October 1, 2009 through
April 30, 2010

We examined the accompanying description of information technology controls applicable to processing transactions for customer organizations using unclassified operating environments administered by the Defense Information Systems Agency (DISA) Computing Services Directorate (CSD) and hosted at the Defense Enterprise Computing Centers (DECCs). The hosting locations are limited to the DECCs in Mechanicsburg, Pennsylvania; and Ogden, Utah; the Infrastructure Service Center (ISC) in St. Louis, Missouri; and the Consolidated Communications Center (CCC) in Montgomery, Alabama; and Oklahoma City, Oklahoma. Our examination included procedures to obtain reasonable assurance about whether:

1. the accompanying description presents fairly, in all material respects, the aspects of DISA CSD's controls that may be relevant to a customer 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 customer organizations applied the controls contemplated in the design of DISA CSD's controls; and
3. such controls had been placed in operation as of April 30, 2010.

DISA CSD uses one subservice organization, which is listed in Section II, including the services it provides. DISA CSD uses a subservice organization for the transport and storage of backup media at an off-site location. The accompanying description includes only those control objectives and related controls of DISA CSD management and does not include control objectives and the related controls of the subservice organization.

We performed our examination in accordance with standards established by the American Institute of Certified Public Accountants and Government Auditing Standards

established by the Comptroller General of the United States, and we included those procedures that we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

Tests of Design of Controls

System Software Changes

As discussed in its description, DISA CSD maintained various aspects of the system software environment in accordance with agreements established with customer organizations. However, DISA CSD did not have the ability to generate automated audit trails of system software changes and thus could not perform periodic reviews to determine whether the changes were authorized. Further, DISA CSD had not defined minimum requirements for documenting (1) details that describe system software changes or (2) system software change testing activities.

As a result, the design of controls is not suitable and does not provide reasonable assurance that the following control will be achieved.

“Controls provide reasonable assurance that changes to system software are authorized, tested, properly implemented in accordance with management's defined requirements, and documented.”

Logical Access

As discussed in its description, DISA CSD conducted various activities in support of its role as administrator of logical access to the system software environment. These activities, however, did not include either a formal process for this role or monitoring tool(s) required to conduct reviews of relevant security event data.

As a result, the design of controls is not suitable and does not provide reasonable assurance that the following control will be achieved.

“Controls provide reasonable assurance that logical access to in-scope systems is granted to properly authorized individuals.”

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of DISA CSD's controls that had been placed in operation as of April 30, 2010. 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 customer organizations applied the controls contemplated in the design of DISA CSD's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Section III, to obtain evidence about their effectiveness in meeting the related control objectives during the period from October 1, 2009 through April 30, 2010. The specific controls and the

nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to customer organizations of DISA CSD and to their auditors, to be taken into consideration, along with information about the internal control at customer organizations, when making assessments of control risk for customer organizations.

Effectiveness of Controls

During tests to obtain evidence about the effectiveness of the controls, listed in Section III, we noted the following deficiencies.

System Software Changes

DISA CSD stated in its description that it had controls in place to restrict the ability to apply changes to the system software environment to authorized users based on job responsibility and the security concept of “least privilege.”¹ However, our tests of operating effectiveness noted that the ability to apply changes to the system software environment was granted to users who did not require such access based on their job responsibilities and least privilege.

Furthermore, as described in the paragraphs preceding our opinion of the suitability of the design of the controls, our tests of design noted a number of additional exceptions that resulted in other system software change management controls not operating effectively. Collectively, as a result, the control is not operating effectively and does not provide reasonable assurance that the following control will be achieved.

“Controls provide reasonable assurance that changes to system software are authorized, tested, properly implemented in accordance with management's defined requirements, and documented.”

Logical Access

DISA CSD stated in its description that it had controls in place to restrict privileged access levels based on job responsibility and least privilege. However, our tests of operating effectiveness noted that these privileged access levels had been assigned to users who did not require such access based on the security concept of least privilege. Other tests of operating effectiveness we performed noted a number of additional exceptions that, in the aggregate, contributed to other logical access controls not operating effectively. Finally, as described in the paragraphs preceding our opinion of the suitability of the design of the controls, our tests of design noted there was a lack of processes and monitoring tool(s) required to effectively review system-generated audit trails for potential security events.

¹ DOD Instruction (DODI) 8500.2, *Information Assurance Implementation*, defines “least privilege” as, “access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization.”

As a result, the control is not operating effectively and does not provide reasonable assurance that the following control will be achieved.

“Controls provide reasonable assurance that logical access to in-scope systems is granted to properly authorized individuals.”

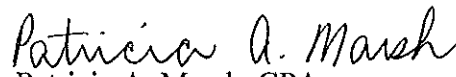
In our opinion, except for the matters described in the paragraphs above, the controls that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period from October 1, 2009 through April 30, 2010.

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

The description of controls at DISA CSD is as of April 30, 2010, and information about tests of the operating effectiveness of specific controls covers the period from October 1, 2009 through April 30, 2010. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at DISA CSD is subject to inherent limitations, and accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such conclusions.

The information in Section IV of this report is presented by the DISA CSD to provide additional information and is not a part of the DISA CSD's description of controls placed in operation. The information in Section IV has not been subjected to the procedures applied in the examination of the description of the controls applicable to the processing of transactions for customer organizations, and accordingly, we express no opinion on it.

This report is intended solely for the information and use of DISA management, its customer organizations, and the independent auditors of its customer organizations and is not intended to be, and should not be, used by anyone other than these specified parties.


Patricia A. Marsh, CPA
Assistant Inspector General
Defense Business Operations

**Section II: Description of the Defense Information Systems
Agency Operations and Controls Provided by the Defense
Information Systems Agency**

II: Description of the Defense Information Systems Agency Operations and Controls Provided by the Defense Information Systems Agency

Overview of Operations

Defense Information Systems Agency

The Defense Information Systems Agency (DISA) is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric² solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other Department of Defense (DOD) Components, under all conditions of peace and war. DISA is the provider of global net-centric solutions for the nation's warfighters and all those who support them in the defense of the nation. The core services are Acquisition, Enterprise Services, Network Operations, Network Services, Net-Centric Enterprise Services, and Global Information Grid (GIG) Bandwidth Expansion. The Field Security Operations (FSO), under the GIG Operations Directorate, and other DISA organizations are included only as they support the Computing Services Directorate (CSD).

Computing Services Directorate

CSD provides computer processing for the entire range of combat support functions, including transportation, logistics, maintenance, munitions, engineering, acquisition, finance, medicine, and military personnel readiness. With more than 3 million users, CSD operates more than 1,400 applications in 18 geographically separate facilities using more than 35 mainframes and more than 6,000 servers. The supported applications:

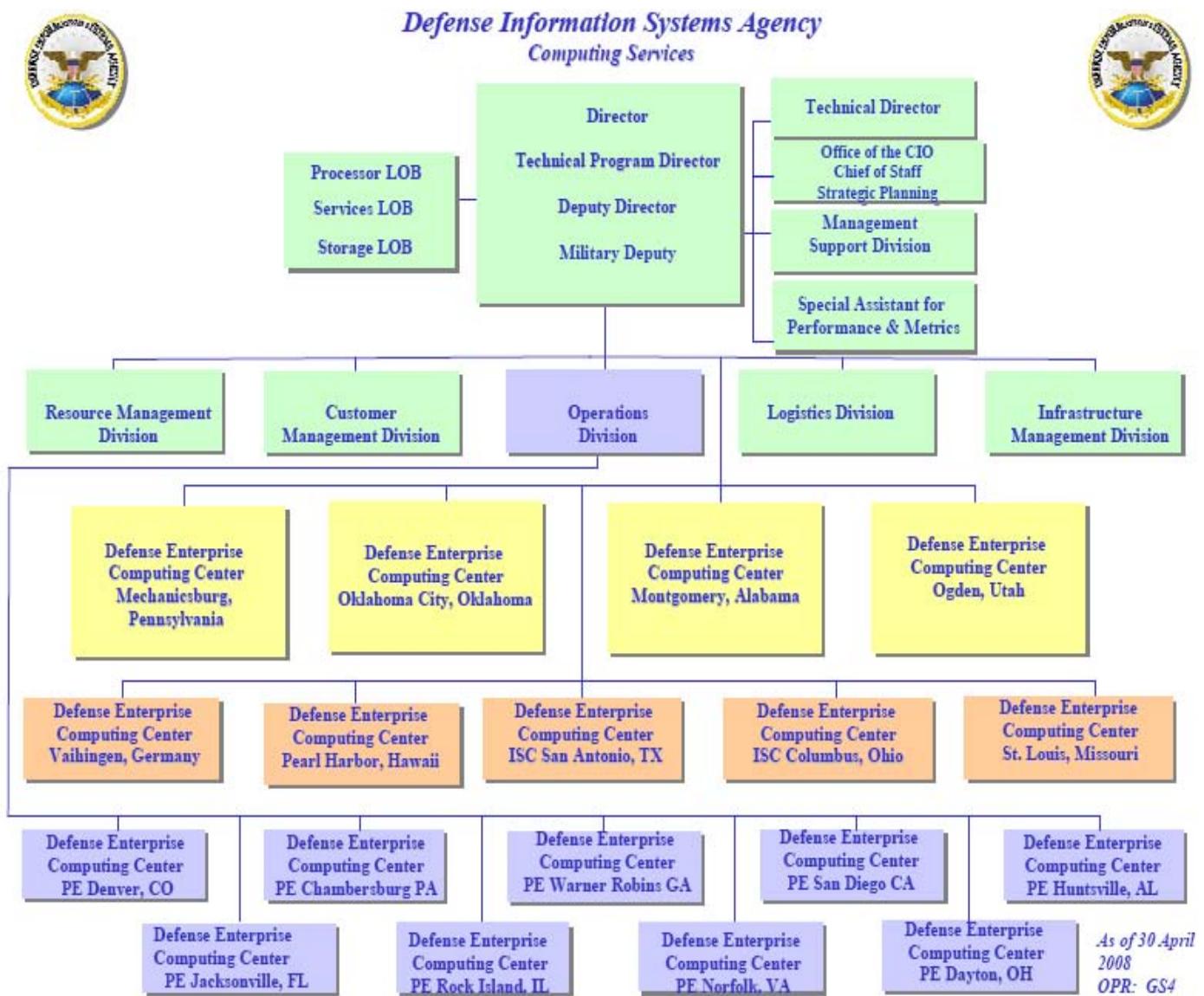
- provide command and control of warfighting forces,
- facilitate the mobility of the war fighters through maintenance of the airlifted and tanker fleets,
- provide war fighter sustainment through resupply and reorder, and
- manage the medical environment and patient care.

CSD features diverse locations, a defense-in-depth philosophy, and dual high-capacity Defense Information Systems Network connectivity. CSD also uses automated systems management to control computing resources and realize economies of scale. CSD has adopted assured computing philosophies and has implemented initiatives in the Unisys and IBM mainframe environments to ensure that information and mission-critical applications are continuously available to customer organizations. Such initiatives include facility upgrades, improved software and equipment availability, diverse and redundant communications, and

² A continuously evolving, complex community of people, devices, information, and services interconnected by a communications network to achieve optimal benefit of resources and better synchronization of events.

measures to remotely replicate data. Assured computing, coupled with the ability to rapidly increase processing and storage capacity via utility contracts, enables DISA to provide the availability and surge capabilities that customer organizations require.

CSD supports computing operations on both DISA-owned and customer organization-owned platforms. Computing services include computer operations, data storage, systems administration, security management, capacity management, system engineering, Web and portal hosting, architectural development, and performance monitoring. Computing services are provided by a highly skilled workforce and performed in state-of-the-art computing facilities strategically located throughout the continental United States (CONUS); Stuttgart, Germany; and Pearl Harbor, Hawaii. DISA facilities operate 24 hours a day, 7 days a week, 365 days a year, and support both unclassified and classified computing environments. Services are available to the Services, Defense agencies, and combatant commanders. This chart provides the organizational structure of CSD.



Headquarters

The primary headquarters for DISA CSD is located in Falls Church, Virginia. Other headquarters elements are located in Chambersburg, Pennsylvania; Denver, Colorado; Oklahoma City, Oklahoma; and Pensacola, Florida. DISA CSD is organized into the following five primary divisions.

The Resource Management Division (RMD) serves as the enterprise manager for managerial accounting, budget formulation, rate development, and financial execution management. RMD performs such functions as: budget formulation and execution, workload customer invoicing, fund certification of acquisition documents, capital budgeting, and execution and preparation of the annual customer planning estimates. RMD has four primary locations in Jacksonville, Florida; Chambersburg, Pennsylvania; Denver, Colorado; and Pensacola, Florida.

The Customer Management Division (CMD) provides the total life cycle management of all customer workload support, including requirements definition, engineering, proposal development, acquisition, implementation, Service Level Agreements (SLAs), as well as billing and invoicing. The CMD also performs the full range of customer relation functions for CSD and coordinates customer related issues with other DISA organizations. CMD is a virtual organization with personnel located in Falls Church; Denver; Chambersburg; Mechanicsburg, Pennsylvania; Oklahoma City; Montgomery, Alabama; Ogden, Utah; and San Antonio, Texas.

The Operations Division advises the Director of CSD on all principal operations and has the overall responsibility for issuing operations and security standards, policies, plans, standard business processes, and standard operating procedures. This division:

- tasks other CSD elements as required to achieve the CSD mission;
- manages and assesses operations and security of all assigned DISA information processing, communications, and network systems;
- provides appropriate assets in response to contingencies and exercises;
- oversees the overall operational performance and effectiveness of the Defense Information Infrastructure efforts implemented within CSD as well as assigned systems;
- develops and maintains CSD programs for configuration management, executive software, capacity management, incoming projects, and contingency operations; and
- manages the Network Operations for CSD and integrates it into the DISA Network Operations program.

The Operations Division is organized in three layers—headquarters-level policy and plans, headquarters-level centralized operations, and direct operations. The direct operations layers include the operating sites and the Consolidated Communication Centers (CCCs).

Operating Sites

The operating sites are called Defense Enterprise Computing Centers (DECCs). The DECCs located outside the continental United States are DECC Pacific in Pearl Harbor and DECC Europe in Stuttgart. They provide processing services for DOD elements within their theater of operations. The DECCs in CONUS are divided into the following mission configurations:

- **System Management Centers (SMCs).** The primary responsibility of each SMC is systems management and customer support functions for the mainframe and server computing environments. The SMCs are located in Mechanicsburg; Montgomery; Ogden; and Oklahoma City.
- **Infrastructure Service Centers (ISCs).** The ISCs perform system management for service-based applications and other specialized fielding efforts from CSD customers. The ISCs are located in Columbus, Ohio; St. Louis, Missouri; and San Antonio, TX.
- **Processing Elements (PEs).** The primary responsibilities for each PE are touch labor³ or “lights dim” components, facility management, hardware support, physical security, touch labor for communication devices, and touch labor for media management. The PEs are located in Chambersburg; Dayton, Ohio; Denver; Huntsville, Alabama; Jacksonville, Florida; Norfolk, Virginia; Rock Island, Illinois; San Diego, California; and Warner Robins, Georgia.
- **Consolidated Communication Centers (CCC).** The primary responsibility of CCC is to manage all classified and unclassified network devices. The CCC is located at SMCs in Montgomery and Oklahoma City.

The Logistics Division supports the Director of CSD on all logistics, acquisition, maintenance, and property management activities and provides command direction and guidance to execute integrated logistics support for assigned activities and systems. This division has offices in Chambersburg and Denver and liaison officers at each SMC.

The Infrastructure Management Division plans, engineers, and maintains the fundamental, non-revenue producing elements required by the DECCs to perform operational processing in support of customer applications. This division:

- provides planning, acquisition, configuration, and quality/risk management for infrastructure initiatives;
- provides Level III communications troubleshooting and complex problem management for the enterprise;
- develops tactical plans and engineers/implements solutions for future technologies;

³ Touch labor refers to personnel providing physical on-site work needed when systems are remotely managed.

- engineers and deploys a standard communications, hardware, software, and enterprise systems management architecture to ensure interoperability; and
- provides tactical and long-range facilities planning for DISA processing sites.

This division has offices in Falls Church, Denver, Pensacola, and Chambersburg.

Information Assurance Support

Almost all DISA elements interact with CSD to some degree. The following DISA elements have a direct relationship with CSD on Information Assurance (IA).

Chief Information Officer

The Chief Information Officer (CIO) provides staff support in accomplishing Information Resource Management (IRM) duties, mandated by the Clinger-Cohen Act. The CIO develops IRM and Information Technology (IT) policies, performs IT management and strategic planning, develops and evaluates IT investment criteria, and incorporates and disseminates architecture and standards guidance. The CIO advises on acquisitions for DISA IT and coordinates with the Office of the Secretary of Defense on IRM, IT, and IT acquisition matters. The CIO is the Designated Approving Authority (DAA) for DISA-owned and operated internal IT enclaves and networks. The CIO manages the agency-wide programs for Privacy Act and records management, manages implementation of electronic business and electronic commerce for DISA, and provides support for DOD Information Assurance Awareness training.

Field Security Operations

FSO provides functional Information Assurance Manager (IAM) services to CSD. The mission of FSO is to provide information systems, network security products, and direct funding and reimbursable services throughout DOD, including the combatant commands, the Services, and Defense agencies. The FSO supports the National Command Authority, combatant commanders, Joint Task Force-Global Network Operations, the Services, and Defense agencies through Global Network Operations, Computer Emergency Response Capabilities, and Information System Security Services. FSO provides such support by directing, managing, and protecting critical elements of the GIG. In this capacity, FSO is the Certifying Authority for the DISA DAA. FSO:

- develops, implements, and maintains security guidance and processes;
- conducts full scope security reviews;
- provides security training, security training products, and system administrator (SA) certification; and
- implements security architecture and IA tools.

Manpower, Personnel, and Security

The Manpower, Personnel, and Security (MPS) Directorate provides plans, programs, and oversight worldwide in the mission areas of civilian personnel, military personnel, human resource development, organization and manpower program administration, payroll, travel,

transportation, mail management, visual information, security, and command information. In addition to worldwide responsibilities, MPS is responsible for providing direct service support to all DISA activities in the National Capital Region.

The Civilian Personnel Division, within MPS, advises and assists the Director of DISA in formulating, executing, and evaluating civilian personnel plans and programs; provides technical guidance and assistance to the DISA managers and employees; and oversees DISA civilian personnel management activities worldwide. The DISA Security Division, within MPS, provides security policy, guidance, and oversight (except for Information Systems Security) to DISA activities worldwide, using a multi-disciplined risk management approach. This division also provides traditional security assistance in information, personnel, physical and special security reviews, and assessments in support of the DISA Security Certification and Accreditation process.

Procurement Directorate

The Procurement Directorate has four contracting organizations. One of the four Defense Information Technology Contracting Organization is located at Scott Air Force Base in Illinois. It supports DISA CSD and is responsible for the procurement of commercial information technology services and equipment required by DOD agencies and other U.S. Government agencies.

Control Environment

IA controls are layered and applied through procedures and physical applications. Controls are employed to protect resources from theft, loss, damage, inadvertent disclosure, compromise, and deliberate attempts to gain access by forced or surreptitious means. Protection is accomplished through the employment of countermeasures to deter, delay, detect, assess, and respond to unauthorized activity.

CSD has the responsibility of providing core services and meeting the CSD customer expectations through professional and consistent operations services and standard implementation of DOD regulations and DOD policies. CSD is responsible for continual refinement and analysis of operations performance metrics and practices to identify and implement opportunities for improvement in the execution of core operations services. CSD is also responsible for maintaining the integrity of the security posture of the operations environment.

Security Management

Security Review Program Guidance

In general, security review programs focus on management actions that establish the DAA and the processes that support the accreditation of an Automated Information System. DOD implemented the Office of Management and Budget Circular A-130, "Management of Federal Information Resources," February 8, 1996, requirements for a security program through DOD certification and accreditation (C&A) and other DOD policies. DISA Instruction 630-230-19, "Automated Data Processing Information Assurance," March 2, 2007, prescribes policy and assigns responsibilities for implementing, managing, and maintaining the DISA Information

Systems Security Program and implements the DOD programs, including the C&A process and designation of DAA. The C&A program is a major component of DISA's security review program.

Security Control Program at the DECCs

DISA CSD Security Handbook, the Information Assurance Vulnerability Alert Handbook, and Security Technical Implementation Guidelines (STIGs) primarily cover the Office of Management and Budget, DOD, and DISA requirements for the primary operational level guidance for implementation of automated information system security controls. The DECC security management organization structure and general business practices support the security program, including review of security controls.

Security Roles and Responsibilities

DISA DAA/CIO

The DISA DAA/CIO retains the overall responsibility for the C&A as it pertains to the DOD C&A process of the CSD sites.

CSD IAM

The CSD IAM function/services are contracted to and performed by the FSO. The CSD IAM provides guidance and direction to field units and advice to CSD on IA, communications, and emanations security. The CSD Chief of Operations and the CSD Chief of Security oversee and ensure delivery of CSD IAM functions/services by FSO.

CSD Security Manager (SM)

The CSD SM function/services are provided to CSD by MPS. The functional CSD SM provides guidance and direction to field units and advice to physical, industrial, personnel, and information security as well as security management. The CSD Chief of Operations and the CSD Chief of Security oversee and ensure delivery of CSD SM functions/services by MPS.

Site IAM

The site IAM develops and maintains an organization or DOD information system-level IA program that identifies IA architecture, requirements, and objectives, in addition to policies, personnel, processes, and procedures. Depending upon the site, the IAM reports to the Chief of Security, the Deputy Director, or the Director of the site.

Site Information Assurance Officer (IAO)

The site IAO assists the IAM in meeting the duties and responsibilities outlined above. The site IAO reports to the IAM of the site.

Risk Assessments

CSD has implemented a risk assessment process to identify and manage risks that could affect customer organizations. This process requires a formal risk assessment, which is part of the

Authority to Operate (ATO). The process also includes an external and internal compliance validation and procedures to maintain an acceptable level of risk.

Formal Risk Assessment

The FSO prepares the formal risk assessment for each CSD site. The threat is determined by validating countermeasures that have been implemented to determine the residual risk. Various tools are used to validate the effectiveness of the implemented countermeasures, including the Security Readiness Review (SRR) and the vulnerability scan used to determine the effectiveness of the network, systems, physical, personnel, information, and industrial security procedural countermeasures. These are conducted by the FSO or as self-assessments performed by site personnel. Environmental and facility reviews conducted by CSD Facility Engineers are used to determine the effectiveness of facility and environmental countermeasures. Various Federal Emergency Management Agency Web sites are used to determine weather, climatic, and natural threats.

The IAMs for DECCs are responsible for reviewing and identifying pen and pencil changes to risk assessment documents on an annual basis. If there are no changes noted, the formal risk assessment document is not re-dated or re-signed. The CSD IAM is responsible for reviewing and making changes to the DECC PEs risk assessment documents as they occur. The formal risk assessment is a required appendix to the ATO under the C&A process by DISA DAA who is the DISA CIO. A complete formal review and documented risk assessment is only conducted every three years.

Mission Assurance Category

The Mission Assurance Category (MAC) reflects the importance of information relative to the achievement of DOD goals and objectives, particularly the war fighter combat mission. MAC levels are the basis for determining availability and integrity control requirements. DOD has three defined MAC levels.

- **MAC I.** This MAC is used to describe systems handling information that is vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.
- **MAC II.** This MAC is used to describe systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance.
- **MAC III.** This MAC is used to describe systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss

of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

Information and Communication

Information Systems Overview

The concept of operations for CSD emphasizes and describes a “customer focused” environment, organized with SMCs, Operational Support Teams, and production operations environments designed to provide a problem resolution and a situational awareness posture over all domains of a dynamic production environment that is operational 24 hours a day, 7 days a week, and 365 days a year. CSD customer support demands include multiple classifications of secure environments, multi-vendor UNIX environments, Intel-based server environments, IBM and Unisys mainframe environments, multiple commercial database environments, commercial off-the-shelf applications, government off-the-shelf applications, customized legacy systems, Web-based systems, voice-based systems, including commercial telephone switch support, Private Branch Exchange support, and multiple communications infrastructures. CSD must have knowledge of the products, services, and applications used by its customer base, as well as information regarding the internal health of the CSD IT environment to provide professional, knowledgeable, and proactive support.

Communication

CSD has implemented various methods of communication to ensure that all employees understand their individual roles and responsibilities. These methods include New Employee Orientation, Individual Development Plans, CSD Plans of the Week that summarize various significant events, and the use of electronic mail messages to communicate time-sensitive messages and information. The Director of CSD holds a weekly staff meeting with all CSD Division Chiefs. All site Chiefs also hold periodic staff meetings as appropriate. Every employee within CSD has a written position description, and every position description includes details of what responsibilities are required of the individual. The CSD Business Management Center is responsible for headquarters level customer relations and acts as the face to the customer. Each operating site within CSD maintains detailed records of problems reported by customer and problems or incidents noted during processing and monitor such items until they are resolved. The Liaison Officer is responsible for the up-channel reporting of operations incidents. Categories of incidents have been identified as high impact, high-visibility, or high-interest requiring detailed reporting to a defined chain of senior management.

Specific information requirements have been defined for the incident reports to help ensure completeness, accuracy, and understandability. Standard trouble tickets that provide the basic information must be cleansed to ensure that these informational requirements are met and consolidated into the defined incident reporting format.

Monitoring

Compliance Validation

DISA compliance validation is conducted externally by the FSO and within CSD using the FSO Toolkits for compliance with the GS4 Letter of Instruction 08-03, "Mandatory Information Assurance Guidance," June 6, 2008. The results from the FSO review are maintained in the Vulnerability Management System (VMS). FSO categorizes the vulnerabilities into four categories, based on severity.

- **Finding Category I.** Any vulnerability that may result in a total loss of information or provide an unauthorized person or software immediate access into a system, gains privileged access, bypasses a firewall, or results in a denial of service.
- **Finding Category II.** Any vulnerability that provides information that has a high potential of giving access to an unauthorized person, or provides an unauthorized person the means to circumvent security controls.
- **Finding Category III.** Any vulnerability that provides information that potentially could lead to an unauthorized access.
- **Finding Category IV.** Any vulnerability that is all other possibilities that contributes to degraded security.

External Compliance Validation

The external compliance validation is conducted by the FSO. Because of the number and size of the sites, a complete review of each site cannot be made on an annual basis. The complete review is conducted during a three-year cycle to coincide with the formal accreditation cycle. Per the DOD C&A requirements, accreditation decisions are made for a maximum of a three-year period. Annual reviews conducted by the FSO are known as Information Assurance Reviews (IARs). The IAR includes a review of the output from the FSO Toolkits, documentation in VMS, manual checklists where toolkits are not available, and a vulnerability or penetration scan. All IAR results are entered into VMS and used by the DISA CIO for the accreditation decision. There are several components to the IAR:

- **Traditional Review.** The traditional review determines whether policies and procedures on physical, information, personnel, industrial, communications, and emanations security comply with DOD regulations and DISA instructions. It also validates whether policies and procedures are correctly and adequately implemented.
- **Technical Review.** The technical review uses a combination of automated and manual checks for network devices, operating systems, databases, and Web applications to verify that configuration settings are in accordance with the applicable STIGs.
- **Vulnerability Scan.** The vulnerability scan process utilizes a commercial automated scanning tool that checks for known vulnerabilities. The scan is a two-step process. The first step is external to the perimeter of the enclave and determines the robustness of perimeter defenses. The second step is internal to the perimeter of the enclave and determines the robustness of the defense of each device within the enclave. In

accordance with Compliance Task Order 08-005, internal scan results are imported into VMS on a monthly basis.

Internal Compliance Validation

The internal validation process is enforced via the Mandatory Information Assurance Guidance, GS4 Letter of Instruction 08-03. This process requires that devices are approved prior to connecting to the network, using the FSO Toolkits and checklists as self-assessments performed by the sites. These results are imported or entered into VMS.

Vulnerability Management System

VMS is a DOD vulnerability management system for Information Assurance Vulnerability Management (IAVM) and STIG compliance. The IAVM portion is used to track acknowledgement and compliance with alerts, bulletins, and technical advisories as directed by Chairman of Joint Chiefs of Staff Instruction 6510-01D, "Information Assurance (IA) and Computer Network Defense." Information for all assets is registered in VMS including system details, operating systems, owner, and managing site. There is a Plan of Action and Milestone (POA&M) process for vulnerabilities that cannot be remediated within the established timeframe. POA&Ms are documented within VMS. The CSD IAM reviews the POA&Ms and concurs/non-concurs. The CIO has the final approval for any POA&Ms. VMS also notifies the managing system administrators (SAs) via email of any newly released IAVMs. The STIG portion identifies vulnerabilities and tracks remediation of those vulnerabilities.

Global Information Grid Monitoring

There are network Intrusion Detection Systems (IDSs) located on the GIG that monitor standard security policy. The GIG network IDSs, monitored by Global Network Security Center (GNSC), are known as the Joint Intrusion Detection System. The GNSC monitors all Joint Intrusion Detection System on the GIG within the CONUS. There are various other centers located around the world, and all centers feed into a DOD Global Network Operations Center. This group identifies any information threat on an isolated, regional, or global basis. The GNSC notifies all parties of any type of potential unauthorized attack or access, and works with the managing CCC and site IA staff to help identify, isolate, investigate, and remediate potential threats.

CSD Enclave Perimeter Monitoring

All CSD enclave perimeters have a layered defense that consists of Access Control Lists on the perimeter router, firewalls, and a network IDS. The security staff located in the CCC develops the security profiles for the enclave perimeter router, perimeter firewall and perimeter network IDSs and monitor their respective reports and audit logs for unauthorized access or activities. This is for the entire CONUS-based CSD network. The security staff located at DECCs Europe and Pacific perform the same tasks locally for their respective enclave perimeter devices. Suspected incidents are investigated in concert with trusted agents from the customer base or data owners to determine the legitimacy of the incidents. If the suspected incident cannot be validated as authorized, they are reported to the Liaison Officer and to the GNSC. The GNSC then directs all actions for this incident and closes it or turns it

over to the appropriate investigative agency for action. The Computing Service Cell reports the incident to CSD Issue Center within the CSD Operations Division.

Enclave Monitoring

The Host-Based Security System solution is in place across the CSD environment for any assets on the Out-of-Band network. Some sites also use a host-based IDS. Validated unauthorized privileged accesses are reported up the same chain as other incidents.

FSO Monitoring

The FSO conducts external vulnerability scanning once a year for the Non-Classified Internet Protocol Router Network and Secret Internet Protocol Router Network connections at all sites. If the scan does not penetrate or identify a weakness in the enclave perimeter, the scan is terminated. If the scan does identify a weakness in the enclave perimeter, the scan continues to further identify weaknesses. The results are entered into VMS and are briefed to the site director and senior staff.

Control Activities

The control objectives provided by and related controls provided by DISA are included in Section III of this report, "Control Objectives, Control Activities, and Tests of Operating Effectiveness." Although the control objectives and related controls are included in Section III, they are an integral part of DISA's descriptions of controls.

User Organization Control Considerations

The DISA control structures are designed to enable user organizations to implement controls that conform to their internal policies, procedures, and internal control requirements. The application of specified controls at user organizations is necessary to achieve the control objectives included in this report.

This section describes the controls that user organizations may need to complement the controls at DISA. The user organization's control considerations presented below should not be regarded as a comprehensive list of all the controls that user organizations should employ. User organization auditors should consider whether the following controls have been placed in operation at user organizations. Although DISA has designed control procedures that are intended to provide effective control over transaction processing, they cannot be expected to develop control procedures to address all contingencies, nor are they able to prescribe or perform the required user procedures that must take place at the user organizations. With these limitations in mind, the following user organization considerations have been presented to help user organizations address control issues that are an integral part of the entire control environment under which their data are processed.

User organizations are responsible for the development, implementation, documentation, review, and modification of appropriate internal control procedures to confirm that data processing by applications hosted in DISA-maintained operating environments is performed completely, accurately, and in a timely manner. Some of the controls that user organizations may be responsible for include, but are not limited to, the following.

Change Management

User organizations should ensure that system software installations, upgrades, and patches are reviewed, tested and approved in accordance with internal procedures as well as the agreed upon division of responsibility between the user organization and DISA for such activities.

Access to Programs and Data

User organizations should ensure that the following controls over logical security have been placed into operation for relevant aspects of their systems in accordance with applicable Federal rules and regulations, internal user organization procedures as well as the agreed upon division of responsibility between the user organization and DISA for such activities:

- Requests for user organization personnel access to user organization-operated applications are documented, reviewed, and approved by user organization management. Approvals and the granting of such access should be issued in consideration of least-privilege and need-to-know security principles.
- Access to user organization-operated applications belonging to separated and transferred user organization employees and contractors is disabled or removed in a timely manner.
- Access to user organization-operated applications is reviewed by management on a periodic basis, and any unauthorized/inappropriate access identified during the review exercise is updated in a timely manner.
- Activity of user organization system administration and security administration accounts is reviewed on a periodic basis, and any suspicious activity is followed up in a timely manner.
- Access to user organization-operated applications is configured with unique user IDs and passwords that are not shared.
- Terminals, Personal Computers (PCs), and so forth are logged off when not in use.
- Password and account security controls are implemented, including those related to password length, complexity, resetting and reuse, and account lockout. Specifically, such configurations should be set in accordance with applicable Federal rules and regulations or the user organization's security policy, whichever is more restrictive. Security configurations should be reviewed on a periodic basis in order to determine continued compliance with policy/minimum requirements.

In consideration of the user organization control considerations above, user organizations should ensure that access to terminals, PCs, and so forth. is restricted to authorized users to the extent feasible. The following should be considered in addressing this control consideration:

- Restriction of physical access to terminals through the use of locked doors, key access, and/or other means.
- Requirements that user organization personnel sign off of their terminals, PCs, and so forth, during lunch hours and other periods of time when the system, terminal, PC, and so forth is not in use.

User organizations should ensure that physical access to computer equipment, storage media, and user documentation at the user organization is limited to properly authorized individuals.

Computer Operations

If DISA's services were temporarily unavailable due to system or communications failures, user organizations could expect some delay before systems are recovered. User organizations should develop procedures to support continued operations during this interim period. These procedures should be documented, tested, and updated periodically.

User organizations should ensure procedures have been placed into operation for the maintenance and preservation of all data files, report files, and programs resident on their in-house systems, such as end user computing applications (user-driven spreadsheets, databases, etc.) that are used in support of related business activities. Procedures should be in place to safeguard primary and backup media from accidental destruction or deletion.

User organizations should ensure that DISA is promptly notified of events that may prohibit the complete, accurate, and timely completion of processing and backups including, but not limited to, problems with system functionality, performance/response and telecommunications.

User organizations should ensure that records are retained for an appropriate time period as designated by applicable laws, rules, regulations, and user organization documentation retention requirements.

User organizations should ensure that data transmissions are complete, accurate, and secure.

Business and Application Processing

User organizations should ensure the following:

- Transactions are authorized, then completely and accurately inputted.
- Changes to static/reference data are authorized, then completely and accurately inputted.
- Changes to existing applications are authorized and tested.
- Changes to existing applications have a documented back-out plan.
- Input is validated by personnel independent of the input function.
- As determined necessary, interim application processing results and/or outputs are reviewed for completeness, accuracy, and validity, and exception items are followed up and resolved on a timely basis.

End User Computing

User organizations should ensure that the environment is suitable for complete, accurate, and authorized end user computing (for example certification of end users, centralized logging of end user application software, and regular management monitoring of end user processing).

Training

User organizations should ensure that staff training and additional training needs are reviewed and implemented on a periodic basis.

Organization and Management

User organizations should ensure that instructions and information provided to DISA are in accordance with the provisions of the servicing agreement with Memorandum of Understanding, Memorandum of Agreement, SLA, or other applicable documents between DISA and the user organization.

Subservice Organizations

Not Subject to Examination

DISA uses subservice organizations to perform a range of functions. The following table describes the subservice organization used.

Subservice Organization	Function
Iron Mountain	Provides offsite storage of media, including backup tapes

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

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

Control Objective 1: Entity-Wide Security Program - Controls provide reasonable assurance that an enterprise-wide security program has been established, approved by management, is monitored and tested, and is maintained.

Related Federal Information Systems Control Audit Manual (FISCAM) Control Objective(s): Establish an entity-wide security management program.

Control Activity	Test Performed	Results of Testing
<p>An agency/entity-wide security management program has been developed and documented that:</p> <ul style="list-style-type: none"> covers all major facilities and operations, has been approved by management, and covers the following elements of a security management program: <ul style="list-style-type: none"> periodic risk assessments, policies and procedures, subordinate information security plans, security awareness training, management testing and evaluation, a remedial action process, security-incident procedures, and continuity of operations. <p>The agency/entity-wide security management program is updated to reflect current conditions.</p>	<p>Inspected the documents comprising the security management program to determine whether it:</p> <ul style="list-style-type: none"> covered all major facilities and operations, had been approved by management, and covered the following elements of a security management program: <ul style="list-style-type: none"> periodic risk assessments, policies and procedures, subordinate information security plans, security awareness training, management testing and evaluation, a remedial action process, security-incident procedures, and continuity of operations. <p>Inspected dates and management sign-offs for the documents comprising the security management program to determine whether they had been recently updated to reflect current conditions.</p>	No exceptions noted.
<p>Enclave security plans have been documented and implemented that:</p> <ul style="list-style-type: none"> cover all major facilities and operations, have been approved, and cover relevant topics prescribed by certification and accreditation policy. 	<p>For DECC Mechanicsburg, DECC Ogden, and ISC St. Louis, inspected the enclave security plans to determine whether they:</p> <ul style="list-style-type: none"> covered all major facilities and operations, had been approved, and 	No exceptions noted.

Control Activity	Test Performed	Results of Testing
Enclave security plans are updated annually or whenever there are significant changes to the agency/entity policies, organization, IT systems, facilities, applications, weaknesses identified, or other conditions that may affect security.	<ul style="list-style-type: none"> covered relevant topics prescribed by certification and accreditation policy. <p>For each plan noted in the procedure above, inspected the supporting documentation to determine whether it was updated within the past year or because of recent significant changes.</p>	
Security control policies and procedures are documented, approved by management, and periodically reviewed and updated.	Inspected selected policies and procedures, and, as applicable, related documentation, to determine whether they were documented, approved by management, and periodically reviewed and updated.	No exceptions noted.
An ongoing security awareness program has been implemented that includes security briefings and training that is monitored for all employees and contractors (collectively referenced as 'staff') with system access and security responsibilities.	<p>Inspected the security awareness training materials to determine whether they have been documented.</p> <p>For a sample of staff, inspected corresponding training management system records to determine whether sampled staff received security awareness training.</p> <p>Inspected documentation evidencing tracking of security awareness training completion to determine whether staff compliance with security awareness training requirements was monitored.</p>	No exceptions noted.
<p>Self-assessments are conducted at the site locations including, but not limited to, a variety of techniques, including the performance of SRR scripts, network scans, and traditional audit procedures to determine the IA posture of new, existing and updated operating environments relative to new, existing, and updated security policy requirements. Self-assessments are scheduled to help ensure that each device is assessed once every 365 days.</p> <p>Vulnerabilities identified through assessments and the related POA&Ms are documented within VMS.</p>	For a sample of mainframe Logical Partitions (LPARs), Windows, and UNIX operating environments, inspected the corresponding vulnerability and POA&M reports from VMS and, as applicable, site-specific tracking documents, to determine whether self-assessments were completed and issues were followed up/remediated.	No exceptions noted.
The FSO performs various independent evaluation techniques including, but not limited to, the	For the projects performed by the FSO at DECC Ogden, DECC Mechanicsburg and ISC St. Louis	No exceptions noted.

Control Activity	Test Performed	Results of Testing
performance of SRR scripts, network scans, and traditional audit techniques in support of the certification and accreditation process. Vulnerabilities identified and associated remediation plans are recorded in VMS, reviewed and approved by management, and tracked through resolution.	during the reporting period, inspected the corresponding FSO-issued site compliance reports and POA&M testing documents to determine whether the reviews were performed and issues were followed up/remediated.	
Action plans and milestones to correct deficiencies are documented.	For DECC Ogden, DECC Mechanicsburg, ISC St. Louis, and the CCC, inspected the corresponding POA&M reports output from VMS to determine whether they were documented to evidence tracking of the remediation of issues.	No exceptions noted.

Control Objective 2: Risk Assessments - Controls provide reasonable assurance that risk assessments are performed and management reviews and addresses risks.

Related FISCAM Control Objective(s): Controls provide reasonable assurance that risks are periodically assessed and validated.

Control Activity	Test Performed	Results of Testing
Risk assessment policies and procedures are documented.	Inspected risk assessment policies and procedures to determine whether they were documented.	No exceptions noted.
Site-level risks are reassessed on a periodic basis or whenever systems, applications, facilities, or other conditions change.	For DECC Ogden, DECC Mechanicsburg, and ISC St. Louis, inspected evidence of the most recently completed risk assessments to determine whether: <ul style="list-style-type: none"> the risk assessment was documented, risks were identified and evaluated (mitigating actions/other determinations were identified/made); risk mitigation plans were documented and tracked; and the above was reviewed and approved by management. 	No exceptions noted.
Changes to systems, facilities, or other conditions and identified security vulnerabilities are analyzed to determine their impact on risk and the	Inquired of management to obtain an understanding of changes to systems, facilities, or other conditions and identified security vulnerabilities	No exceptions noted.

Control Activity	Test Performed	Results of Testing
risk assessment is performed or revised as necessary.	<p>requiring consideration during the risk assessment process.</p> <p>Inspected the most recently completed risk assessments to determine whether changes to systems, facilities, or other conditions and identified security vulnerabilities were analyzed to determine their impact on risk and the risk assessment is performed or revised as necessary.</p>	
DISA enclaves are certified and accredited before being placed in operation and at least every three years, or more frequently if major system changes occur.	<p>For DECC Ogden, DECC Mechanicsburg, and ISC St. Louis, inquired of management and inspected related C&A completion schedules (or equivalent documentation) to obtain an understanding of:</p> <ul style="list-style-type: none"> • each site's annual/triennial C&A due date, • whether each site has recently undergone a significant change, and/or • each site's completion status of ongoing C&A activities, as applicable. <p>For DECC Ogden, DECC Mechanicsburg, and ISC St. Louis, inspected the most recently completed enclave C&A package (including the ATO or equivalent decision document and risk analysis documentation) to determine whether the C&As were performed and documented, including applicable risk assessment processes.</p>	DECC Ogden operated without an enclave ATO or Interim Authority To Operate during the period of April 5, 2010, through April 15, 2010. The previous Interim Authority To Operate expired on April 4, 2010.

Control Objective 3: Personnel Procedures - Controls provide reasonable assurance that Government employees and contractors (collectively referenced as ‘staff’) undergo required clearance procedures prior to receiving system access, terminated staff are out-processed in accordance with applicable Federal and DOD requirements, and job descriptions are documented.

Related FISCAM Control Objective(s): Controls provide reasonable assurance that security management is effective, including effective:

- *hiring, transfer, termination, and performance policies address security, and*
- *[policies and procedures that help ensure that] employees have adequate training and expertise.*

Control Activity	Test Performed	Results of Testing
The completion of staff background investigations is validated before they are given authorization to access organizational information and information systems.	For a sample of staff with privileged access to the in-scope systems, inspected the corresponding user access forms to determine whether the completion of a background investigation was verified before the access was provided.	No exceptions noted.
Periodic reinvestigations are performed as required by law for employees, and implementing regulations at least once every 10 years, consistent with the sensitivity of the position.	For a sample of employees whose investigation expired during the reporting period, inspected the Joint Personnel Adjudication System records to determine whether such activities were completed.	MPS did not maintain evidence that background reinvestigations for 2 of 40 staff members selected for review were initiated once every five years as required by the policy.
Nondisclosure agreements are required for staff.	For a sample of staff hired during the reporting period, inspected the corresponding nondisclosure agreements to determine whether they were completed.	No exceptions noted.
As applicable, termination and transfer procedures include: <ul style="list-style-type: none"> • exit interview procedures; • return of property, keys, identification cards, passes, etc.; • notification to security management of terminations and revocation of IDs and passwords; • immediate escort of terminated staff out of the agency’s facilities; and • identification of the period during which nondisclosure requirements remain in effect. 	<p>For a sample of terminated and transferred staff during the reporting period, inspected the corresponding exit checklists to determine whether they were completed (indicating timely completion of out-processing activities).</p> <p>For the same sample of terminated and transferred staff, inspected the corresponding facility and data center access listings generated from the physical access systems to determine whether physical access was deleted or disabled.</p> <p>For the same sample of terminated and transferred staff, inspected the corresponding system-generated</p>	DECC Mechanicsburg did not revoke physical access to the facility or the internal data center for one of 10 terminated staff members selected for review until 83 days after the employee’s separation from DISA.

Control Activity	Test Performed	Results of Testing
	operating system access listings to determine whether logical access was deleted or disabled.	
Skill needs are accurately identified and included in job descriptions, and employees meet these requirements.	For a sample of employees, inspected the corresponding position descriptions and performance evaluations (and, if needed, inquired of them/their supervisor) to determine if their job responsibilities were accurately described in their position descriptions, and the employees met the requirements of the position descriptions.	No exceptions noted.

Control Objective 4: System Software Maintenance - Controls provide reasonable assurance that changes to system software⁴ are authorized, tested, properly implemented in accordance with management's defined requirements, and documented.

Related FISCAM Control Objective(s): Controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended, including effective:

- *Configuration management policies, plans, and procedures,*
- *[Processes to maintain] Current configuration identification information,*
- *[And] Proper authorization, testing, approval, and tracking of all configuration changes,*
- *Routine monitoring of the configuration,*
- *[Processes to update] Software on a timely basis to protect against known vulnerabilities, and*
- *Documentation and approval of emergency changes to the configuration.*

Control Activity	Test Performed	Results of Testing
The formal change management process is documented.	Inspected DOD, DISA, and site-level policies and procedures to determine whether change management policies and procedures are documented.	No exceptions noted.
Except for relationships in which customer organizations have	Inquired of management to obtain an understanding of nature and extent	DISA CSD management was unable to provide complete system-

⁴ For the purposes of this report, "system software" is defined as the following software components installed on the operating environments included in the scope of the examination:

- Mainframe and mid-tier operating systems software
- Mainframe security packages such as Resource Access Control Facility (RACF), Access Control Facility 2 (ACF2) and Top Secret Security
- UNIX-based security services such as Secure Shell
- Operating system software patches (primarily applicable to Windows and UNIX operating environments)

Control Activity	Test Performed	Results of Testing
<p>assumed responsibility for testing, system software changes (including the installation of new operating environments) are tested and authorized by management.</p>	<p>of system software change logging for the purposes of identifying a population of changes implemented during the reporting period and for performing reviews of system software changes applied to production operating environments to help ensure all changes made are authorized.</p> <p>For a sample of operating system software changes recorded in the site change control tracking systems, inspected corresponding change management record details to determine whether the change was described and management authorization and testing activities were documented in accordance with policy requirements and related agreements between DISA and the customer organizations.</p>	<p>generated audit trails of system software changes. Therefore, we were unable to verify the completeness and accuracy of manually maintained change management records.</p> <p>DISA CSD management does not have a process to periodically review system software changes applied to production operating environments to help ensure all changes made are authorized.</p> <p>DECC Mechanicsburg has inconsistent or no testing documentation for 24 of 69 change management records sampled.</p> <p>(Note: At DECC Ogden and ISC St. Louis, customer organizations assumed responsibility for the completion of system software change testing. As a result, we did not conduct procedures to verify the existence of documentation evidencing the performance of system software change testing.)</p> <p>DISA CSD management has not established standards outlining the minimum documentation requirements to describe system software changes in change management systems. Specifically:</p> <ul style="list-style-type: none"> • DECC Mechanicsburg could not map 59 of 158 IAVM alerts sampled to an associated change management record containing corresponding approvals and testing evidence. • DECC Ogden could not map 19 of 164 IAVM alerts sampled to an associated change management record containing corresponding approvals and testing evidence.
<p>A patch management process is documented and implemented, including:</p> <ul style="list-style-type: none"> • identification of systems affected by recently announced 	<p>For a sample of IAVM bulletins determined to be applicable to a selection of operating environments, inquired of management and inspected the corresponding change management records to determine</p>	<p>DISA management has not established standards outlining the minimum documentation required to describe system software changes in site change management systems. As a result, change management</p>

Control Activity	Test Performed	Results of Testing
<p>software vulnerabilities;</p> <ul style="list-style-type: none"> • prioritization of patches based on system configuration and risk; • testing for effectiveness and potential side effects on related systems (except for relationships in which customer organizations have assumed responsibility for testing); and • verification that patches, service packs, and hot fixes were installed on affected systems. 	<p>whether:</p> <ul style="list-style-type: none"> • the vulnerability was identified and prioritized by site management; • systems affected by recently announced software vulnerabilities were identified; • prioritization of patches based on system configuration and risk was performed; • testing for effectiveness and potential side effects on related systems was performed; and • verification that patches, service packs, and hot fixes were installed on affected systems was performed. 	<p>records were not consistently documented at a sufficient level of detail to enable their tracing to corresponding system changes.</p> <p>DECC Ogden did not install the corresponding patch for one of 164 IAVM alerts sampled on the related operating environment.</p> <p>These inconsistencies prevented site personnel from successfully tracing the IAVM alerts selected for testing to the corresponding change management records. Specifically:</p> <ul style="list-style-type: none"> • DECC Mechanicsburg could not map 59 of 158 IAVM alerts sampled to an associated change management record containing corresponding approvals and testing evidence • DECC Ogden could not map 19 of 164 IAVM alerts sampled to an associated change management record containing corresponding approvals and testing evidence. In addition, for 1 of 164 IAVM alerts, DECC Ogden did not install a patch on the related operating environment.
<p>An emergency change management procedure is documented. Emergency changes are documented, approved, and verified either prior to or as soon after implementation as operationally possible.</p>	<p>Inquired of management to obtain an understanding of nature and extent of system software change logging for the purposes of identifying a population of changes – including those related emergency circumstances– implemented during the reporting period and for performing reviews of system software changes applied to production operating environments to help ensure all changes made are authorized.</p> <p>For a sample of emergency requests, inspected the change records to determine whether the request was described and the approval and testing/verification was documented either prior to or soon after the change was implemented.</p>	<p>DISA CSD management was unable to provide complete system-generated audit trails of system software changes. Therefore, we were unable to verify the completeness and accuracy of manually maintained change management records.</p> <p>DISA CSD management does not have a process to periodically review system software changes applied to production operating environments to help ensure all changes made are authorized.</p> <p>DISA CSD management did not establish standards that outlined the minimum documentation required as evidence for the completion of system software testing activities. As a result, DECC Mechanicsburg</p>

Control Activity	Test Performed	Results of Testing
		<p>has inconsistent or no testing documentation for 24 of 69 change management records sampled.</p> <p>(Note: At DECC Ogden and ISC St. Louis, customer organizations assumed responsibility for the completion of system software change testing. As a result, we did not conduct procedures to verify the existence of documentation evidencing the performance of system software change testing.)</p> <p>DISA CSD management has not established standards outlining the minimum documentation requirements to describe system software changes in change management systems. Specifically:</p> <ul style="list-style-type: none"> • DECC Mechanicsburg could not map 59 of 158 IAVM alerts sampled to an associated change management record containing corresponding approvals and testing evidence. • DECC Ogden could not map 19 of 164 IAVM alerts sampled to an associated change management record containing corresponding approvals and testing evidence.
Access to implement system software changes into the production environment is restricted to staff based on job responsibility and least privilege	For a sample of staff with access to implement system software changes in the selected operating environments, inquired of management and/or inspected DD Form 2875s, organizational charts or position descriptions to determine whether such access was restricted based on job responsibility and least privilege.	<p>DECC Mechanicsburg granted 16 members of the Storage Management team access to the privileged section of ACF2 that allows full access to mainframe datasets and resources. In addition, the Storage Management team had access to the RACF attribute that permits users access to a wide range of system resources, which may include full access to RACF-protected resources. We found that DISA could have assigned more restrictive privileges to avoid granting this level of access.</p> <p>DECC Ogden granted 26 Database Administrators ROOT account passwords to all 24 UNIX operating environments selected for testing.</p>

Control Activity	Test Performed	Results of Testing
		<p>We found that DISA could have assigned more restrictive privileges to avoid granting this level of access.</p> <p>For 2 of the 45 sensitive mainframe datasets selected for testing, ISC St. Louis did not restrict write-level access privileges to users based on job responsibilities and least privilege. Upon notification of the exception, St. Louis management modified the privileges to restrict access based on job responsibility and least privilege.</p> <p>For one of three mainframe LPARs selected for testing, ISC St. Louis did not restrict access to privileged section of ACF2 that allows full access to mainframe datasets and resources based on job responsibility and least privilege. Upon notification of the exception, St. Louis management removed the user's access.</p>

Control Objective 5: Physical Access - Controls provide reasonable assurance that physical access to premises used to host in-scope systems is granted to properly authorized individuals.

Related FISCAM Control Objective(s): Controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals.

Control Activity	Test Performed	Results of Testing
All staff access is authorized and credentials (for example, badges, identification cards, smart cards) are issued to allow access.	For a sample of staff hired during the reporting period who were provided access to the facilities/sensitive areas within, inspected the corresponding access form to determine whether the access was authorized.	No exceptions noted.
Access to facilities and the internally located data center is restricted through the use of gates and fences, security guards, electronic card key systems, and/or keys.	Observed the facility's entrances to note whether the facility was secured using gates and fences, security guards, electronic card key systems, and/or keys.	No exceptions noted.
Sensitive information technology and infrastructure resources maintained in the data center are secured using an	Observed the data center's entrances to note whether the data center is	

Control Activity	Test Performed	Results of Testing
electronic card key system and/or keys.	secured using an electronic card key system and/or keys.	
Access to the internally located data center is limited to those individuals who routinely need access per their job responsibilities and least privilege security principles.	For a sample of staff provided access to the data center, inquired of management and/or inspected organizational charts/position descriptions to determine whether access provided was based on valid job responsibilities and least privilege.	For 9 of 33 staff members selected for review, ISC St. Louis did not document the authorization for physical access to the first floor computer room on the required physical access forms. Upon notification of the exception, ISC St. Louis created physical access forms that included authorizations for access to the first floor computer room for each of the nine staff members.
Annually, management conducts a review of individuals with physical access to the data center to ensure such access remains appropriate per staff's current job responsibilities.	<p>Inspected the evidence of the most recently completed physical security reviews to determine whether the reviews were performed within one year and exceptional access identified during the review was removed or modified as requested by the reviewer.</p> <p>Inspected system-generated access lists and activity reports from DECC Ogden's physical access management system to determine:</p> <ul style="list-style-type: none"> the period of time two staff members retained physical access to the computer room after such access was identified as inappropriate during the most recent annual validation, and whether those staff members used the access in question to the enter the computer room during that time period. 	<p>DECC Ogden did not remove the physical access privileges for two of eight staff members identified as no longer requiring access to the computer room during the most recent annual revalidation until 212 days after the inappropriate access was first identified. <i>(System-generated audit trails from DECC Ogden's physical management system indicated that the inappropriate access was not used during the 212-day period.)</i></p> <p>For 9 of 33 staff members selected for review, ISC St. Louis did not document the authorization for physical access to the first floor computer room on the required physical access forms that served as the evidence of the performance of the most recent annual revalidation of physical access. <i>(Upon notification of the exception, ISC St. Louis created physical access forms that included authorizations for access to the first floor computer room for each of the nine staff members.)</i></p>
Visitor access logs are maintained.	For a sample of dates, inspected the corresponding visitor logs for the facilities/data centers to determine	No exceptions noted.

Control Activity	Test Performed	Results of Testing
	whether the records in the logs were sufficiently complete to provide a record of authorized visitor entry.	
Upon separation, staffs' physical access to sensitive facilities and areas within those facilities is disabled or removed. As possible, corresponding access credentials (e.g., electronic card keys) are recaptured during the out-processing cycle.	For a sample of terminated and transferred staff, inspected the corresponding facility and data center access listings generated from the physical access systems to determine whether physical access was deleted or disabled.	For 1 of 10 terminated staff members selected for review, DECC Mechanicsburg did not revoke physical access to the facility or the internal data center until 83 days after the employee's separation from DISA.

Control Objective 6: Logical Access - Controls provide reasonable assurance that logical access to in-scope systems is granted to properly authorized individuals.

Related FISCAM Control Objective(s): Controls provide reasonable assurance that access to computer resources is reasonable and restricted to authorized individuals, including effective:

- ***Protection of information system boundaries,***
- ***Identification and authentication mechanisms,***
- ***Authorization controls,***
- ***Protection of sensitive system resources, and***
- ***Audit and monitoring capability, including incident handling.***

Control Activity	Test Performed	Results of Testing
Each privileged user identification issued is evidenced by a DD Form 2875 (or its predecessor DISA Form 41) or an equivalent local form that has incorporated all of the requirements of the DD Form 2875. DD Form 2875, System Access Authorization Request, requires approval from the user's supervisor, and validation of user personnel security investigation based on the access requested.	For a sample of staff with privileged access to in-scope systems, inspected the corresponding user access forms to determine whether the access request, authorization, and validation of user personnel security investigation was documented.	No exceptions noted.
Revalidation of access to DISA managed systems is conducted annually by the local IAM/IAO and/or SA to identify privileged accounts and privileged user accesses that are no longer needed. At ISC St. Louis, the DD Form 2875 for each user is reviewed to perform the revalidation, whereas at DECC Ogden and DECC Mechanicsburg, the	Inquired of management to obtain an understanding of how the annual revalidation of access to DISA managed systems was performed. For a sample of staff with privileged access to in-scope systems, inspected the corresponding DD Form 2875s to determine whether a revalidation was performed within a year of testing.	DECC Ogden did not perform a revalidation of access within the past year for one of 45 privileged users selected for review. Upon notification of the exception, management prepared a new DD Form 2875 for the affected user that indicated the access provided was still valid.

Control Activity	Test Performed	Results of Testing
system-generated lists of privileged access are reviewed to perform the revalidation.	Inquired of management and inspected system generated access lists to determine whether the inappropriate access identified during the revalidation was updated.	ISC St. Louis did not revalidate the access rules for each system user during their annual revalidation process. As a result, ISC St. Louis' revalidation process did not consider potentially unauthorized access configured within the systems but not documented on the DD Form 2875 for each user.
Inactive accounts and accounts for terminated individuals are disabled or removed within 2 days of communication of the termination/transfer.	<p>For a sample of terminated and transferred staff, inspected the corresponding system-generated operating system access listings to determine whether logical access was deleted or disabled.</p> <p>For the selected operating environments, inspected configurations controlling the disablement of inactive user IDs to determine whether they were set in accordance with STIGs.</p> <p>For the selected operating environments, inspected system reports to determine if inactive accounts are removed in accordance with STIGs.</p> <p>Testing Technique</p> <p>The testing technique used to identify this exception involved:</p> <p>(1) performing an automated scan that reported the time elapsed since the last use of each of the accounts (i.e., the "inactivity period"),</p> <p>(2) identifying those accounts with inactivity periods greater than 35 days, and</p> <p>(3) inspecting the users' account inactivity settings to confirm they were not configured in accordance with the STIG.</p>	<p>DECC Mechanicsburg did not configure the inactive account check parameter to execute daily as required by the STIG for 1 of the 11 mainframe LPARs selected for testing. Upon notification of the exception, management updated the inactive account check parameter to execute on a daily basis.</p> <p>DECC Ogden did not configure the 'user account inactivity' setting to lock the account after 35 days of inactivity as required by the corresponding STIG⁵ for 125 of the 8,469 accounts set up on six of 24 UNIX operating environments selected for testing. Upon notification of the exception, management updated the user account inactivity setting parameter for each of the 125 accounts to lock the account after 35 days of inactivity.</p>

⁵ The 125 accounts noted in this exception represent approximately 1.48 percent of the total population of 8,469 accounts set up on the 24 UNIX operating environments selected for testing. Based on the testing technique described in the Test Performed column, it is possible that more accounts than the 125 noted in this exception have noncompliant user account inactivity settings.

Control Activity	Test Performed	Results of Testing
	<i>The testing technique was not designed to identify accounts with noncompliant user account inactivity settings that had inactivity periods of less than 35 days.</i>	
Access to sensitive/privileged accounts is restricted to individuals or processes having a legitimate need for the purposes of accomplishing a valid business purpose.	For a sample of user accounts possessing sensitive/privileged access on the selected operating environments, inquired of management and/or inspected DD Form 2875s to determine whether such access was provided to individuals or processes with a legitimate need for the purposes of accomplishing a valid business purpose.	<p>ISC St. Louis did not restrict access to the privileged ACF2 section that allows full access to mainframe datasets and resources for one user based on job responsibility and least privilege for one of three mainframe LPARs selected for testing. Upon notification of the exception, management removed the user's access to the privileged ACF2 section.</p> <p>DECC Mechanicsburg granted 16 members of the Storage Management team the ACF2 privilege that allows full access to mainframe datasets and resources and the RACF privilege that permits users access to a wide range of system resources, which may include full access to RACF-protected resources. We found that DISA could have assigned more restrictive privileges to avoid granting this level of access.</p> <p>DECC Ogden did not restrict access to the ROOT account based on job responsibility and least privilege for 26 Database Administrators for all 24 UNIX operating environments selected for testing. We found that DISA could have assigned more restrictive privileges to avoid granting this level of access.</p>
Emergency accounts are available for use by authorized users. Passwords for emergency accounts are maintained in sealed envelopes, and stored in restricted areas and/or safes. Authorized users must request the password for the emergency account	For a sample of emergency accounts used during the reporting period, inquired of management and inspected the corresponding password log to determine whether the access was recorded and use was by an authorized individual.	No exceptions noted.

Control Activity	Test Performed	Results of Testing
and uses of the account are logged. Passwords are changed upon use of the emergency account.	For the same sample of emergency account uses, inspected the corresponding account configurations and/or password change dates to determine whether the accounts had been restricted/suspended and/or the password had been changed.	
<p>The FSO and sites conduct periodic reviews to determine operating system compliance with current applicable STIGs as applicable related to:</p> <ul style="list-style-type: none"> • password and account settings; • audit logging; • access configurations; and • other critical security settings. <p>Vulnerabilities identified through the reviews and the related POA&Ms are documented within VMS.</p>	<p>For a sample of site reviews performed by FSO during the reporting period, inspected the corresponding evidence of the review to determine whether the reviews and related followup and resolution of identified security weaknesses were completed and documented.</p> <p>For the selection of operating environments, inspected the corresponding evidence of the review to determine whether self-assessments were completed and issues were followed up/remediated.</p>	No exceptions noted.
<p>Operating systems are configured in compliance with current applicable STIGs as applicable related to:</p> <ul style="list-style-type: none"> • password and account settings; • audit logging; • access configurations; and • other critical security settings. 	For the selection of operating environments, inspected system outputs of applicable configuration settings and STIG requirements to determine whether operating systems are configured in accordance with STIGs as applicable.	<p>DECC Mechanicsburg did not configure the following settings in accordance with corresponding STIG requirements:</p> <ul style="list-style-type: none"> • For one of 1,376 accounts on one UNIX Solaris operating environments selected for testing had a password that was set to 'null.' • For 2 of 23 Windows operating environments selected for testing, excessive write access rights to audit logs were identified. Specifically, an administrators group containing the two server system administrators and an application account were granted this access, which is against the STIG requirements. <p>DECC Ogden did not configure the following settings in accordance with corresponding</p>

Control Activity	Test Performed	Results of Testing
		<p>STIG requirements:</p> <ul style="list-style-type: none"> One of 8,469 UNIX accounts selected for testing had an easily guessed password. One of 24 UNIX operating environments' Network Time Protocol daemon was not configured to point to an authoritative local or DOD source. <p>Upon notification of these exceptions, management updated the settings in accordance with the STIG requirements.</p>
<p>Security violations and activities, including failed logon attempts, other failed access attempts, and sensitive activity, are recorded.</p> <p>Requirements to proactively review audit logs according to an established frequency and document such activities have not been formalized through a DISA-wide policy and, as a result, proactive audit log reviews are inconsistently performed/documented across the sites.</p> <p>Further, native operating systems and, as applicable, security utility audit logging capabilities are leveraged to generate significant volumes of logs. DISA does not have a tool to distill relevant security event data from these logs. As a result, site personnel responsible for reviewing log data are faced with significant challenges to perform an effective review.</p> <p>Potential and confirmed security violations and suspicious activity identified are escalated to supervisory and management personnel in accordance with the defined incident reporting process.</p>	<p>Inquired of management to obtain an understanding of processes and controls related to the generation, collection/distillation, review, and follow up of audit trails.</p> <p>For the selected operating environments, inspected system outputs of applicable configuration settings and STIG requirements to determine whether audit trail collection settings are configured in accordance with the STIGs as applicable.</p>	<p>DISA did not have formal requirements to review audit logs according to an established frequency and document such activities. As a result, proactive audit log reviews were inconsistently performed/documented across the sites.</p> <p>DISA did not have a tool to extract relevant security event data from native operating systems and, as applicable, security utility audit logs.</p>
Approved equipment, techniques, and procedures are implemented to clear sensitive data from digital media before its disposal or release for reuse	For a sample of digital media disposals during the reporting period, inspected the corresponding disposal records to determine whether procedures to clear	ISC St. Louis did not create a media disposal log that provided evidence of the degaussing and disposal of unclassified

Control Activity	Test Performed	Results of Testing
outside of the organization.	sensitive data from digital media before its disposal or release for reuse outside of the organization were performed and documented.	magnetic tape media.

Control Objective 7: Network Services - Controls provide reasonable assurance that the network is protected from unauthorized access.

Related FISCAM Control Objective(s): Controls provide a reasonable assurance that networks are configured to adequately protect access paths within and between systems.

Control Activity	Test Performed	Results of Testing
Remote access to the network is restricted. Remote access is approved based on valid business need. Requests for and approval of such access is documented.	For a sample of staff with remote access, inquired of management and inspected the corresponding user access request forms to determine whether access requests and approvals for remote access to the network, and the corresponding business justifications for such access were documented.	DISA did not maintain a corresponding system authorization form documenting authorization for remote access to the Out-of-Band network for 1 of 45 privileged users selected for review. Upon notification of the exception, management removed the user's remote access.
FSO and sites conduct periodic reviews to determine compliance with current applicable STIGs related to the following areas: <ul style="list-style-type: none"> network device configuration; audit logging; access configurations; and other critical security settings. Vulnerabilities identified through the reviews and the related POA&Ms are documented within VMS.	For a sample of site reviews performed by FSO during the reporting period, inspected the corresponding evidence of the review to determine whether the reviews and related followup and resolution of identified security weaknesses were completed and documented. For the selection of operating environments, inspected the corresponding evidence of the review to determine whether self-assessments were completed and issues were followed up/remediated.	No exceptions noted.
Networking equipment is configured in accordance with the current DOD STIGs.	For a selection of network devices, inspected system outputs of applicable configuration settings and STIG requirements to determine whether operating systems are configured in accordance with STIGs as applicable.	No exceptions noted.
Anti-virus software has been deployed to protect systems that are susceptible to virus threats. Up-to-date anti-virus signature files are maintained.	For a selection of operating environments, inspected applicable STIGs and related system configurations to determine whether anti-virus software was implemented	No exceptions noted.

Control Activity	Test Performed	Results of Testing
	and configured in accordance with applicable requirements.	
<p>Procedures are in place for monitoring, investigating and reporting inappropriate or unusual activity.</p> <p>Suspicious access activity is investigated and appropriate action is taken in accordance with incident management policies.</p>	<p>For a selection of network devices, inquired of management and inspected the corresponding audit logs and evidence that such logs were reviewed to determine whether the logs were generated and reviewed in accordance with policy requirements.</p> <p>For a sample of security incidents identified in the sample of logs referenced in the test step above, inquired of management and inspected the corresponding security incident reports to determine whether identified security incidents were investigated and resolved and reported to the appropriate supervisory and management personnel.</p>	No exceptions noted.

Control Objective 8: Physical Environment - Controls provide reasonable assurance that the physical environment is monitored and protected from disruptive events.

Related FISCAM Control Objective(s): Controls provide reasonable assurance that contingency planning (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions occur.

Control Activity	Test Performed	Results of Testing
<p>The following fire detection and suppression systems have been implemented:</p> <ul style="list-style-type: none"> • fire and smoke detection systems configured to alarm locally and/or to the local fire department; • performance of fire inspections in accordance with the rules of the local jurisdiction; • automatically activating fire suppression systems for computing facilities, support areas and selected administrative areas; and • fire extinguishers for other administrative areas. 	<p>Observed the facility and data center and inquired of management to determine whether the following environmental controls were implemented:</p> <ul style="list-style-type: none"> • fire and smoke detection systems configured to alarm locally and/or to the local fire department; • performance of fire inspections in accordance with the rules of the local jurisdiction; • automatically activating fire suppression systems for computing facilities, support areas and selected administrative areas; and • fire extinguishers for other administrative areas. 	No exceptions noted.

Control Activity	Test Performed	Results of Testing
<p>Computer facilities are equipped with the following environmental controls:</p> <ul style="list-style-type: none"> • automatic humidity and temperature control systems that issue an alarm when established humidity and temperature conditions are exceeded; • a master power switch located at or near the main entrance, which is labeled and protected by a cover to prevent accidental shut-off; • automatic voltage control systems that issue an alarm if the voltage fluctuates beyond established safe operational levels; • a minimum of two electrical feeds; • a battery powered Uninterrupted Power System (UPS) to provide sufficient power to all systems in the computer room to allow for at least 20 minutes of operations; and • backup generators that are set to automatically start up and generate power when commercial power fails. 	<p>Observed the data center to note whether the following environmental controls have been implemented:</p> <ul style="list-style-type: none"> • automatic humidity and temperature control systems that issue an alarm when established humidity and temperature conditions are exceeded; • a master power switch located at or near the main entrance, which is labeled and protected by a cover to prevent accidental shut-off; • automatic voltage control systems that issue an alarm if the voltage fluctuates beyond established safe operational levels; • a minimum of two electrical feeds; • a battery powered UPS to provide sufficient power to all systems in the computer room to allow for at least 20 minutes of operations; and • backup generators that are set to automatically start up and generate power when commercial power fails. 	<p>No exceptions noted.</p>
<p>The backup generators are tested monthly for operations and power generations.</p> <p>The backup generator, UPS, air conditioning system and fire suppression systems are inspected and/or undergo regular periodic maintenance to help ensure continued operation.</p>	<p>For a sample of months, inspected the corresponding results of the backup generator tests and, if exceptional results were identified, inquired of management to be informed of the resolution to determine whether the tests were performed and exceptional results were followed up and resolved.</p> <p>Inspected maintenance contracts for environment protection devices to determine whether agreements were in place for the maintenance of the environmental control systems.</p>	<p>No exceptions noted.</p>
<p>Routine periodic preventive maintenance on IT equipment is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the</p>	<p>Inspected the maintenance contracts held by the CSD Logistics Division related to Windows, UNIX, and mainframe-based hardware technologies to determine whether</p>	<p>No exceptions noted.</p>

Control Activity	Test Performed	Results of Testing
impact on operations or as provided for in the maintenance contract.	maintenance agreements that provide for the performance routine/periodic maintenance for IT equipment were in place.	

Control Objective 9: Backup and Recovery - Controls provide reasonable assurance that backup and recovery procedures are available to preserve the integrity of programs and data files.

Related FISCAM Control Objective(s): Controls provide reasonable assurance that contingency planning (1) protects information resources and minimizes the risk of unplanned interruptions and (2)provides for recovery of critical operations should interruptions occur.

Control Activity	Test Performed	Results of Testing
Backup files are recorded to media such as backup tapes on a daily to weekly basis, depending on the platform.	For a selection of operating environments, inquired of management and inspected the applicable backup policies and procedures and backup tool/job/script configurations to determine whether backups are configured to take place in accordance with policy.	No exceptions noted.
Facilities exist for the storage of backup files and backup files are rotated offsite on a daily to weekly basis. These sites are geographically removed from the primary site.	Inspected the contract established with the offsite storage provider to determine whether geographically removed facilities have been provided for the offsite rotation of backup media. For a sample of dates, inspected the corresponding pick up manifests to determine whether the rotation of backup media to the offsite storage location was documented.	No exceptions noted.
Access to recall backup media from offsite facilities is restricted to authorized individuals based on valid job responsibilities and least privilege.	Inquired of management and inspected organizational charts and/or position descriptions and the offsite storage recall list to determine whether access to recall backup media from the offsite location is restricted to authorized individuals based on valid job responsibilities and least privilege.	No exceptions noted.
Access to backup media stored onsite is restricted to authorized individuals based on valid job responsibilities and least privilege.	Inquired of management and inspected organizational charts and/or position descriptions and the system-generated access listing for the location at which backup media is stored onsite to	No exceptions noted.

Control Activity	Test Performed	Results of Testing
	determine whether physical access to backup media stored onsite is restricted to authorized individuals based on valid job responsibilities and least privilege.	
Backup job failures are recorded and tracked through resolution.	For a sample of backup job failures for the selected operating environments, inspected the corresponding work tickets to determine whether backup job failures were recorded and tracked through resolution.	No exceptions noted.

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

Introduction

DISA has prepared this section, and it is included to provide user organizations with information DISA believes will be of interest. However, this information is not covered within the scope or control objectives established for the Statement on Auditing Standards 70 examination. Specifically, this section includes a summary of procedures that DISA implemented to enable it to recover from a disaster affecting DECC Ogden, DECC Mechanicsburg, or ISC St. Louis.

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

CSD Service Continuity Management Program

The CSD Continuity of Operations Plan (COOP)/Service Continuity program is based primarily on achieving regulatory compliance with DOD Instruction (DODI) 8500.2, *Information Assurance (IA) Implementation*, for application protection and recovery, as well as DOD Directive 3020.26, *Department of Defense Continuity Programs*, for continuity of Command and Control and other mission essential functions and services. CSD uses “best practices” defined by the “Professional Practices for Business Continuity Professionals,” as developed by the Disaster Recovery Institute International, the Business Continuity Institute, and the *Disaster Recovery Journal*. The CSD COOP/Service Continuity Team Members (CD514) are certified by the Disaster Recovery Institute International as Business Continuity Planners or are in pursuit of certification.

CSD is a service provider and operates according to SLAs that are negotiated with customers who receive data processing support from DISA. Those SLAs are designed to document customer requirements and DISA obligations in support of those requirements. In the case of COOP/Service Continuity, the customer may have the option, depending upon the processing platform, of requesting COOP support from DISA or satisfying the COOP requirement elsewhere through in-house or third-party strategies. Ultimately, CSD relies on the SLA to ensure that customer expectations and DISA obligations are matched appropriately for both parties.

To that end, if a customer has opted to satisfy the COOP requirement through CSD, then addressing the IA controls from DODI 8500.2 becomes the responsibility of CSD. In that effort, CD514 ensures that a designated alternate site is identified and that documented recovery procedures are developed and, on customer request, that they are exercised. In an effort to ensure compliance with regulatory requirements, CD514 will participate, through the IG office, in addressing questions raised during audits.

If a customer has opted to satisfy its COOP requirements without the involvement of CSD, then the IA controls from DODI 8500.2 remain the responsibility of the customer. CD514 conducts large-scale and ad hoc briefings regularly to increase awareness of the

COOP/Service Continuity program among CSD personnel as well as those groups and organizations that are current or potential customers. Those briefings provide an overview of the program and opportunities for questions and clarification.

In addition to the application-centric exercises driven by customer requests, CD514 conducts a Business Continuity Plan walk-through exercise for each site within CSD. That allows CSD to review and refine the site-based procedures for incident response and the restoration of Command and Control, as well as other recovery topics that may be part of a specific exercise or scenario.

All exercises are facilitated using a formal exercise plan and are documented through the development of After Action Reports, which document action items or issues identified during the exercise. Those items or issues are tracked through the resolution stage by CD514. Through these combined efforts across the enterprise, the COOP/Service Continuity requirements are addressed and the documented processes and procedures are continually refined and confirmed.

Acronyms and Abbreviations

ACF2	Access Control Facility 2
ATO	Authority to Operate
C&A	Certification and Accreditation
CCB	Change Control Board
CCC	Consolidated Communication Center
CIO	Chief Information Officer
CMD	Customer Management Division
CONUS	Continental United States
COOP	Continuity of Operations Plan
CSD	Computing Services Directorate
DAA	Designated Approval Authority
DECC	Defense Enterprise Computing Center
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODI	Department of Defense Instruction
FSO	Field Security Operations
GIG	Global Information Grid
GNSC	Global Network Service Center
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAR	Information Assurance Review
IAVM	Information Assurance Vulnerability Management
IDS	Intrusion Detection System
IRM	Information Resource Management
ISC	Infrastructure Service Center
IT	Information Technology
LPAR	Logical Partition
MAC	Mission Assurance Category
MPS	Manpower, Personnel and Security
PC	Personal Computer
PE	Processing Element
POA&M	Plan of Action & Milestone
RACF	Resource Access Control Facility
RMD	Resource Management Division
SA	System Administrator
SAS 70	Statement on Auditing Standards No. 70
SLA	Service Level Agreement

SM	Security Manager
SMC	System Management Center
SRR	Security Readiness Review
STIG	Security Technical Implementation Guide
UPS	Uninterrupted Power System/Uninterrupted Power Supply
VMS	Vulnerability Management System

~~FOR OFFICIAL USE ONLY~~



Inspector General
Department *of* Defense

~~FOR OFFICIAL USE ONLY~~