Report No. D-2008-138 September 30, 2008

Inspector General
United States
Department of Defense

Defense Information Systems Agency Controls Over the Center for Computing Services Placed in Operation and Tests of Operating Effectiveness for the Period April 1, 2007, through March 31, 2008

Additional Information and Copies

The Department of Defense Office of the Deputy Inspector General for Auditing, Defense Financial Auditing Service prepared this report. If you have questions or would like to obtain additional copies of this report, contact Ms. Patricia C. Remington at (703) 601-5815 (DSN 329-5815) or Mr. Richard Ng at (703) 601-5805 (DSN 329-5805).

Suggestions for Audits

To suggest ideas for or to request future audits, contact the Office of the Deputy Inspector General for Auditing at (703) 604-9142 (DSN 664-9142) or fax (703) 604-8932. Ideas and requests can also be mailed to:

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

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

September 30, 2008

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE
(COMPTROLLER)/CHIEF FINANCIAL OFFICER
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY

SUBJECT: Report on Defense Information Systems Agency Controls Over the Center for Computing Services Placed in Operation and Tests of Operating Effectiveness for the Period April 1, 2007, through March 31, 2008 (Report No. D-2008-138)

We are providing this report for your information and use. No written response to this report is required.

We appreciate the courtesies extended to the staff. Please direct questions to Ms. Patricia C. Remington at (703) 601-5815 (DSN 329-5815) or Mr. Richard Ng at (703) 601-5805 (DSN 329-5805). The team members are listed inside the back cover.

Patricia A. Marsh

Patricia A. Marsh, CPA
Assistant Inspector General
Defense Financial Auditing Service

Table of Contents

FOREWORD

This report is intended for use by Defense Information Systems Agency (DISA) management, its user organizations, and the independent auditors of its user organizations.

The Department of Defense (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, as amended, mandates that agencies prepare and conduct audits of financial statements. The reliability of information processed at the DISA sites directly impact the ability of DoD to produce reliable, and ultimately auditable, financial statements, which is key to achieving the goals of the Chief Financial Officers Act.

This report focuses on the DISA Center for Computing Services (CS). CS provides computer processing for the entire range of combat support functions, including transportation, logistics, maintenance, munitions, engineering, acquisition, finance, medicine, and military personnel readiness. CS offers computing services on CS 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-defined controls over the CS environment. The report provides an opinion on the fairness of the DISA presentation of its description of controls, the suitability of the design of controls, and the operating effectiveness of key controls that are relevant to audits of a user organization's financial statements. As a result, this examination may preclude the need for additional audits of general controls, such as those that user organizations previously performed to plan or conduct financial statement and performance audits. From this examination, we will also provide a separate audit report with recommendations to management for correcting identified internal control deficiencies.

Effective internal control is a critical and required element to achieve reliable information for management reporting and decision making. The concept of adequate internal control is the fundamental objective of this American Institute of Certified Public Accountants Statement on Auditing Standards No. 70 Report. Internal control is a process designed by management to provide reasonable assurance that the activity achieves its objectives related to the reliability of financial reporting, the effectiveness of operations, and compliance with applicable significant laws and regulations. DISA has implemented internal control standards for the CS environment that require strict compliance with DoD and DISA policies. The level of DISA compliance with specific aspects of these regulations has a direct impact on the accompanying description of internal controls and related control test results.

Section I: Independent Service Auditor's Report

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

September 30, 2008

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on Defense Information Systems Agency Controls Over the Center for Computing Services Placed in Operation and Tests of Operating Effectiveness for the Period April 1, 2007, through March 31, 2008 (Report No. D-2008-138)

We have examined the accompanying description of specific information technology related controls of unclassified technologies (operating systems) of the Defense Information Systems Agency (DISA) over selected Defense Enterprise Computing Centers, listed in the Scope appendix on page 69, of the Center for Computing Services (CS). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of controls at DISA over CS that may be relevant to a user organization's internal control as it relates to an audit of financial statements, (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and user organizations applied the controls contemplated in the design of controls at DISA, and (3) such controls had been placed in operation as of March 31, 2008. The control objectives were specified by the management of DISA. Our examination was performed 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 included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

As discussed in the accompanying description of controls, CS did not have control procedures in place to ensure that responsibilities of security officials at all levels were defined in the DISA Computing Services Enterprise Security Roles and Responsibilities Concept of Operations. In addition, DISA did not have control procedures in place to ensure security awareness completion was recorded and maintained in the Defense On-Line Training System. These deficiencies resulted in controls not being suitably designed to achieve Control Objective 4, "Controls provide reasonable assurance that a security management structure is established and security responsibilities are clearly assigned."

As discussed in the accompanying description of controls, CS did not have control procedures in place to ensure that passwords were configured in accordance with DoD Security Technical Implementation Guides and all access paths have been identified and controls implemented to prevent and detect access. These deficiencies resulted in controls not being suitably designed to achieve Control Objective 9, "Controls provide reasonable assurance that adequate logical access controls have been implemented."

As discussed in the accompanying description of controls, CS did not have control procedures in place to ensure that audit trails were being maintained and reviewed. This resulted in controls not being suitably designed to achieve Control Objective 11, "Controls provide reasonable assurance that access is monitored, suspected security violations are investigated, and appropriate remedial action is taken."

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of controls that had been placed in operation as of March 31, 2008. Also, in our opinion, except for the deficiencies in the design of the controls and their effect on the related control objectives described in the preceding paragraphs, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of the CS 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 our description of the tests of operating effectiveness, to obtain evidence about their effectiveness in meeting the related control objectives, described in Section III of this report, during the period from April 1, 2007, to March 31, 2008. The specific controls and the nature, timing, extent, and results of the tests are listed in our description of the tests of operating effectiveness. This information has been provided to user organizations of CS and to their auditors to be taken into consideration, along with information about the internal control at user organizations, when making assessments of control risk for user organizations.

In our opinion the controls that were tested, as presented in our description of the tests of operating effectiveness, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in our description of those tests were achieved during the period from April 1, 2007, to March 31, 2008.

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

The description of the controls over CS is as of March 31, 2008, and information about tests of the operating effectiveness of specific controls covers the period from April 1, 2007, to March 31, 2008. 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 the service organization 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 CS to provide additional information to user organizations and is not part of the description of controls placed in operation provided by CS. The information in Section IV has not been subjected to the procedures applied in the examination of the description of controls applicable to the processing of transactions for user organizations, and accordingly we express no opinion on it.

This report is intended solely for the management of CS, its users, and the independent auditors of its users.

Patricia A. Marsh

Patricia A. Marsh, CPA
Assistant Inspector General
Defense Financial Auditing Service

Section II: Information Provided by DISA

2007 SAS-70

Statement on Auditing Standards

Section II

A. Overview of Operations

Defense Information Systems Agency

Defense Information Systems Agency (DISA) is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric[1] 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 war fighters 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 Office (FSO), under the GIG Operations Directorate, and other DISA organizations are included only as they support Center for Computing Services (CS).

Center for Computing Services

CS 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 3,000,000 users, CS operates over 1,400 applications in 18 geographically separate facilities utilizing more than 35 mainframes and more than 6,000 servers. The supported applications: 1) provide command and control of war fighting forces, 2) facilitate mobility of the war fighters through maintenance of the airlifted and tanker fleets, 3) provide war fighter sustainment through resupply and reorder, and 4) manage the medical environment and patient care.

[1] 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.

CS features diverse locations, a defense-in-depth philosophy, and dual high-capacity Defense Information Systems Network (DISN) connectivity. CS also utilizes automated systems management to control computing resources and realize economies of scale. CS 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 customers. Such initiatives include facility upgrades, improved software and equipment availability, diverse and redundant communications, and 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 customers require.

CS supports computing operations on both DISA-owned and customer-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); Vaihingen, Germany; and Pearl Harbor, Hawaii. DISA facilities are operational 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. Chart 1 provides the organizational structure of CS.

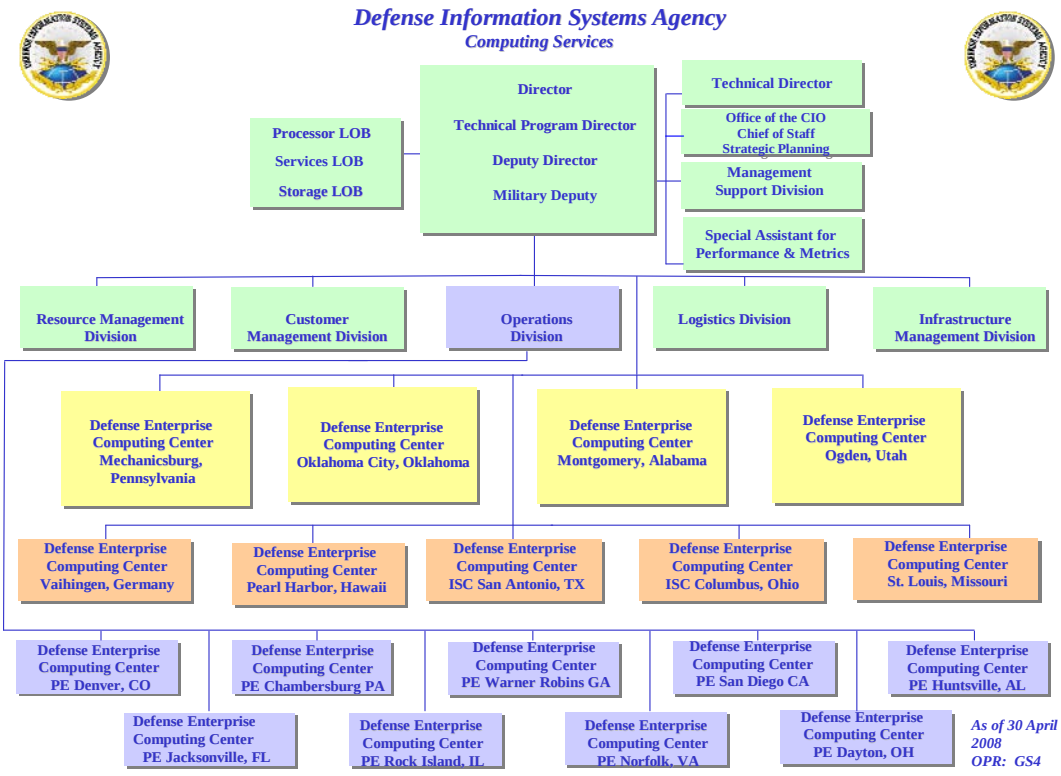

Chart 1

Headquarters. The primary headquarters for DISA CS is located in Falls Church, VA. There are other headquarters elements located in Chambersburg, PA; Denver, CO; Oklahoma City, OK and Pensacola, FL. CS is organized into the following five primary divisions.

Resource Management Division. 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 is located at four primary locations: Jacksonville, FL; Chambersburg, PA; Denver, CO; and Pensacola FL.

Customer Management Division. 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 CS and coordinates customer related issues with other DISA organizations. CMD is a virtual organization with personnel located in Falls Church, VA; Denver, CO; Chambersburg, PA; Mechanicsburg, PA; Oklahoma City, OK; Montgomery, AL; Ogden, UT; and San Antonio, TX.

Operations Division. The Operations Division advises the Director of CS 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 CS elements as required to achieve the CS 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 (DII) efforts implemented within CS as well as assigned systems;
- develops and maintains CS programs for configuration management, executive software, capacity management, incoming projects, and contingency operations; and
- manages the Network Operations for CS 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 Communications Control 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, Hawaii and DECC Europe in Stuttgart, Germany. They provide processing services for DoD elements within their theater of operations. The DECCs in CONUS are divided into the following mission configurations:

1) **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, PA; Montgomery, AL; Ogden, UT and Oklahoma City, OK.

2) **Infrastructure Service Centers (ISCs).** The ISCs perform system management for service-based applications and other specialized fielding efforts from CS customers. The ISCs are located at Columbus, OH, St. Louis, MO and San Antonio, TX.

3) **Processing Elements (PEs).** The PEs serve as touch labor[2] or "lights dim" components, facility management, hardware support, physical security, touch labor for communication devices, and touch labor for media management are the primary responsibilities for each PE. The PEs are located in Chambersburg, PA; Dayton, OH; Denver, CO; Huntsville, AL; Jacksonville, FL; Norfolk, VA; Rock Island, IL; San Diego, CA and Warner Robins, GA.

4) **Central Communication Centers (CCCs).** The primary responsibility of CCCs are to manage all classified and unclassified network devices. The CCCs are located at SMCs in Montgomery, AL and Oklahoma City, OK.

Logistics Division. The Logistics Division supports the Director of CS 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, PA, Denver, CO and liaison officers at each SMC.

Infrastructure Management Division (IMD). The IMD 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;

[2] 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, VA, Denver, CO, Pensacola, FL, and Chambersburg, PA.

Information Assurance Support

Almost all DISA elements interact with CS to some degree. The following DISA elements have a direct relationship with CS 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, strategic planning, 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 CS. 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 (JTF-GNO), the Services, and Defense agencies through Global Network Operations, Computer Emergency Response Capabilities, and Information System Security Services. The FSO provides such support by directing, managing, and protecting critical elements of the GIG. In this capacity, the FSO is the Certifying Authority for the DISA DAA. The 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 information assurance (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 and 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 is the Defense Information Technology Contracting Organization located at Scott Air Force Base, Illinois. It supports CS and is responsible for the procurement of commercial information technology services and equipment required by DoD agencies and other U.S. Government agencies.

B. Overview of Control Environment

IA controls are layered and are 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.

CS has the responsibility of providing core services and meeting the CS customer expectations through professional and consistent operations services and standard implementation of DoD regulations and DoD policies. CS 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. CS 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 (AIS). DoD implemented the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources", February 8, 1996, requirements for a security program through DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," 28 November 2007, and other DoD policies. DISA Instruction 630-230-19, "Automated Data Processing Information Assurance", 2 March 2007, prescribes policy and assigns responsibilities for implementing, managing, and maintaining the DISA Information Systems Security Program and implements the DoD programs, including DIACAP and designation of DAA. The DIACAP and resultant

Certification and Accreditation (C&A) program are major components of DISA's security review program.

Security Control Program at the DECCs. DISA CS Security Handbook; the Information Assurance Vulnerability Alert Handbook; and Security Technical Implementation Guidelines (STIGs), primarily cover the OMB, DoD, and DISA requirements for the primary operational-level guidance for implementation of AIS security controls. The DECC security management organization structure and general business practices support the security program, including review of security controls.

Security Roles and Responsibility

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

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

CS Security Manager (SM). The CS SM function/services are provided to CS by Manpower, Personnel and Security (MPS). The functional CS SM provides guidance and direction to field units and advice to physical, industrial, personnel, and information security as well as security management. The CS Chief of Operations and the CS Chief of Security oversee and ensure delivery of CS 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, objectives, and policies; personnel; and 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

CS 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 System Security Authorization Agreement (SSAA). 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 CS 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 can be conducted by the FSO or as self-assessments performed by site personnel. Environmental and facility reviews conducted by

CS Facility Engineers are used to determine the effectiveness of facility and environmental countermeasures. Various Federal Emergency Management Agency (FEMA) 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 CS 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 SSAA under the DIACAP 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**. 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.** 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**. 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.

Compliance Validation

DISA compliance validation is conducted externally by the FSO and within CS using the FSO Toolkits for compliance with the GS4 Letter of Instruction (LOI) 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 which 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 DIACAP, 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 (IAW) the applicable STIGs.

- **Vulnerability Scans**. 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. IAW Compliance Task Order (CTO) 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 LOI 08-03. This process ensures devices are approved prior to connecting to the network,

using the FSO Toolkits and checklists as a self-assessment. 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: 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. The CS 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.

GIG 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), is (are) known as the Joint Intrusion Detection System (JIDS). The GNSC monitors all JIDS 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 (GNOC). 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 Information Assurance (IA) staff to help identify, isolate, investigate, and remediate potential threats.

CS Enclave Perimeter Monitoring

All CS enclave perimeters have a layered defense that consists of Access Control Lists (ACLs) on the perimeter router, firewalls, and a network IDS. The security staff located in the CCCs 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 CS network. The security staffs 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 (LNO) 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 (CSC) reports the incident to CS Issue Center within the CS Operations Division.

Enclave Monitoring

Host Based Security System (HBSS) is currently being deployed across the CS environment for any assets on the Out of Band (OOB) 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 (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) 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.

Segregation of Duties

Segregation of duties is handled IAW the DISA CS Security Handbook.

Personnel Controls

All personnel must meet employment requirements and are subject to a favorable personnel security investigation. An authorization document, known as the Joint Table of Distribution (JTD) authorizes all Government (civilian and military) positions. This document also identifies the sensitivity, IT level, and security clearance requirement for each position. These three elements determine the type of investigation required and the type and frequency of periodic reinvestigations.

All personnel are subjected to various levels of personnel security investigation, which is based on the level of privileges they have within systems. All personnel possess Secret clearance with IT-2 level, except for those with privileged access (SAs, Database Administrators (DBAs), Storage Administrators, Network Administrators, etc.) The SAs are required to have Secret clearance with IT-1 level. All personnel security is managed and monitored by DISA MPS6 in concert with site SMs. The CS SM submits all personnel security actions through DISA MPS6. The DISA Security Office issues requests for additional information, intent to deny or revoke, and actual revocations of security clearances or favorable investigations.

Environmental Controls

The Facilities Engineering Branch, a CS Headquarters organization in Denver establishes facility standards for the DECCs on electrical distribution, Uninterrupted Power Supply (UPS), fire detection and fire suppression, and climate control IAW national standards.

- **Electrical Distribution**. Most sites have at least two electrical power feeds either from the installation or another commercial source. There are automatic voltage controls at all computing facilities and alerts of any potential electrical problems. There is a master power switch located at the primary entrances in all computer facilities.

- **UPS**. Each site has an UPS consisting of constantly charged batteries in case of power disruption. The UPS is constantly monitored and alerts staff of any potential problem.

Each site is also equipped with generators that provide an automatic start-up power source. Backup power sources are tested on a periodic basis to ensure that they function properly and provide sufficient electrical power to meet site operating requirements. Additional fuel is stored on site for sustained backup operations. The fuel is tested on an annual basis for contamination.

- **Fire Detection**. Most administrative areas are protected by fire detection systems that alarm either locally or at a responding fire department. All computing facilities are protected by automatic fire detection systems that alarm at the responding fire department.

- **Fire Suppression**. All administrative areas are protected by either automatic or manual fire suppression systems. All computing facilities are protected by automatic fire detection systems (smoke or fire detectors) that respond to heat or smoke to suppress fires. Fire prevention is an inherent responsibility of every CS employee and requires alertness and cooperation from all individuals and agencies that may be in the building. Each site follows the facility emergency plan for the protection of all Government employees and private industry tenants.

- **Climate Control**. There are mechanical systems that provide the constant and desired temperature, humidity, and air particles. The climate control system is constantly monitored and alerts of any potential problem. Many of the computer facilities are equipped with water detection systems and a water drainage system to handle excess water under the raised floor area.

Physical Security Controls

- **Administrative Areas**. All buildings and administrative areas have limited entry points and all are protected by automated access card systems or by guards located at the entrances. In some cases, both are used; guards protect the area during normal duty hours from Monday through Friday, and the automated access card system controls access during all off-duty hours. All personnel must wear identification badges while in the area. Visitors to all sites must be signed into the administrative area and obtain local badges that must be displayed while in the buildings. The issuance of an escort-required or a non-escort required visitor badge depends on the validation of visitor's investigation type and security clearance.

- **Computer Facility**. All computer facilities have implemented the following physical controls:

    - controlled access and controlled perimeter for CS facilities located on a military or General Services Administration (GSA) installation;
    - verification of DoD identification such as a Common Access Cards or DISA badge;
    - enclosed perimeter by a fence that controls vehicle and pedestrian access for facilities not located on a military or GSA installation;

- routine patrol and random door checks performed by local military, DoD, or GSA guards in accordance with the local base support agreement; and
- access to the administrative areas controlled by guard, mechanical cipher, or automated access control system.

- **Facility Support Areas**. Access to facility support areas is controlled either by fencing, automated access control systems, or key locking devices. These areas are not considered "Restricted Areas". Most of the facilities have closed circuit television coverage of all doors to computer facilities, buildings, and facility support areas inside and outside of the buildings. A local guard monitors the cameras at some sites. Where cameras are not monitored, access is recorded and surveillance tapes are maintained for at least 30 days.

- **Information Security Controls.** Only properly cleared personnel with a need-to-know are granted access to classified information. All classified paper documents are stored in an approved GSA security container. Combinations to approved storage areas and security containers are restricted to only those who need to gain access, and a Standard Form (SF) 700 identifies who holds the combinations. The combination is treated as classified information and must be located in another security container. All security containers and approved storage areas must have a SF 702 on the outside and must be annotated with the initials of the person opening the containers as well as the date and time the container was open and closed. Security containers are to be inspected daily and annotated on the SF 702 to prevent security breach.

  All classified transmissions that egress the perimeter router are encrypted using National Security Agency (NSA) Type I encryption devices and keying material. In some cases, transmissions inside the enclave are not encrypted but are required to be in an appropriate Protected Distribution System (PDS). The Federal Information Processing Standards (FIPS) 140-2, "Security Requirements for Cryptographic Modules", released May 25, 2001, requires that encryption be used to protect the transmission of unclassified information, when required by the customer in the SLA. All computing areas that process classified information must be in an approved classified information storage area or continuously be manned by properly cleared personnel who can observe every device (computing and networking) processing classified information. Unless requested by the customer, all information stored on magnetic media is not encrypted. NSA devices are used for classified information and FIPS 140-2 compliant devices are used for unclassified information. All classified and unclassified information must be destroyed using approved methods of destruction IAW DoD Regulation 5200.1-R, "Information Security Program", January 1997.

Industrial Security Controls

Contracts must address security requirements. The contract should identify:

- the requirement for IT level and the personnel security investigation;

- the requirement for the contractor to provide visit request information for all contractor personnel that need to visit a Government location;

- the requirement to comply with all security policies and procedures at Government locations;

- the configuration requirement for contractor-provided equipment that will be connected to Government networks and enclaves, if no Government-furnished equipment is provided; and

- the requirement for a DD Form 254, for contracts that require access to classified information, that outlines the required level of security clearance, where classified information can be accessed, and any special instructions.

C. Information and Communication

Information Systems Overview

The concept of operations for CS emphasizes and describes a "customer focused" environment, organized with SMCs, Operational Support Teams (OSTs), 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. CS 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 (COTS) applications, Government Off-The-Shelf (GOTS) applications, customized legacy systems, web-based systems, voice-based systems including commercial telephone switch support, Private Branch Exchange (PBX) support, and multiple communications infrastructures. CS must have knowledge of the products, services, and applications used by its customer base, as well as information regarding the internal health of the CS IT environment to provide professional, knowledgeable, and proactive support.

Communication

CS has implemented various methods of communications to ensure that all employees understand their individual roles and responsibilities. These methods include New Employee Orientation, Individual Development Plan (IDP), CS Plan of the Week that summarizes various significant events, and the use of electronic mail messages to communicate time-sensitive messages and information. The Director of CS holds a weekly staff meeting with all CS Division Chiefs. All site Chiefs also hold periodic staff meetings as appropriate. Every employee within CS has a written Position Description (PD), and every PD includes details of what responsibilities are required of the individual.

The CS Business Management Center (BMC) is responsible for headquarters level customer relations and acts as the face to the customer. Each operating site within CS maintains detailed records of problems reported by customer and problems or incidents noted during processing and monitor such items until they are resolved. The LNO 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.

D. Control Objectives and Related Control Activities

CS control objectives and related controls are included in Section III, "Control Objectives, Controls Activities, and Tests of Operating Effectiveness," of this report to eliminate the redundancy that would result from listing them in this section and repeating them in Section III. Although the control objectives and related controls are included in Section III, they are nevertheless, an integral part of CS control descriptions.

E. User Control Considerations

Computing Services User Controls

CS and its customers share the controls over the users. This shared environment normally is delineated between the computing environment and the applications.

Customer User Controls

Customers are expected to have general user controls, at a minimum, built into their applications and should be delineated in the application SSAA documentation.

SLAs

An SLA is a contract between a service agency and a customer agency that defines the parameters of the services. The SLA defines the services to be delivered, problem management, and customer duties and responsibilities. The SLA outlines, at a minimum, the responsibilities over system access, security controls, data disposition and sharing, data encryption, and data backup for both CS and the customers.

F. Acronyms

ACL	Access Control List
AIS	Automated Information System
BMC	Business Management Center
C&A	Certification and Accreditation
CAC	Common Access Card
CCC	Central Communication Center
CIO	Chief Information Officer
CMD	Customer Management Division
CONUS	Continental United States
COTS	Commercial Off-The-Shelf

CS	Computing Services
CSC	Computing Service Cell
CTO	Compliance Task Order
DAA	Designated Approving Authority
DBA	Database Administrator
DECC	Defense Enterprise Computing Center
DIACAP	DoD Information Assurance Certification and Accreditation Process
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FSO	Field Security Office
GIG	Global Information Grid
GNOC	Global Network Operations Center
GNSC	Global Network Security Center
GOTS	Government Off-The-Shelf
GSA	General Services Administration
HBSS	Host Based Security System
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAR	Information Assurance Review
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
IDP	Individual Development Plan
IDS	Intrusion Detection System
IMD	Infrastructure Management Division
IRM	Information Resource Management
ISC	Infrastructure Service Center
IT	Information Technology
JIDS	Joint Intrusion Detection System
JTD	Joint Table of Distribution
JTF-GNO	Joint Task Force-Global Network Operations
LNO	Liaison Officer
LOI	Letter of Instruction
MAC	Mission Assurance Category
MPS	Manpower, Personnel and Security
NIPRNET	Non-Classified Internet Protocol Router Network
NSA	National Security Agency
OMB	Office of Management and Budget
OOB	Out of Band
OST	Operational Support Team
PBX	Private Branch Exchange
PD	Position Description

PDS	Protected Distribution System
PE	Processing Element
POA&M	Plan of Action and Milestone
RMD	Resource Management Division
SA	System Administrator
SF	Standard Form
SIPRNET	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SM	Security Manager
SMC	System Management Center
SRR	Security Readiness Review
SSAA	System Security Authorization Agreement
STIG	Security Technical Implementation Guideline
UPS	Uninterrupted Power Supply
VMS	Vulnerability Management System

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

Security Program

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
1	**Controls provide reasonable assurance that the security program effectiveness is monitored and changes are made as needed.**			
1.1	Management periodically assesses the appropriateness of security policies and procedures.	SP5.1 Annual reviews are conducted to accommodate new security policy requirements, technology changes, etc. checked by the Information Assurance Review (IAR) process.	We requested documentation of the annual review that accommodates new security policy requirements, technology changes, and related changes. We reviewed the CSD IAM description of the annual review process.	CSD IAM did not conduct annual reviews to accommodate new security policy requirements and technology changes.
		SP5.1 CS Operations Division conducts annual reviews to assess the appropriateness of the CS security policies.	We requested documentation of the CS Operations Division annual review that assesses the appropriateness of the CS security policies. We reviewed the CS Operations Division description of the annual review process.	CS Operations Division did not conduct annual reviews to assess the appropriateness of the CS security policies.
		SP5.1 The FSO conducts annual Technical Interchange Meetings to assess the appropriateness of the security policies.	We reviewed the Technical Interchange Meetings (TIMs) minutes the FSO prepared to determine whether the FSO assessed the appropriateness of the security policies.	No relevant exceptions noted.
1.2	Management monitors compliance with policies and procedures.	SP5.2 FSO performs SRRs as part of the IA review and certification and accreditation process.	We inspected SRRs that we obtained from the FSO to determine whether the FSO performed the SRRs.	No relevant exceptions noted.
		SP5.2 CSD IAM provides weekly report on IAVMs to CSD Senior Management.	We inspected a sample of 14 weekly Information Assurance Vulnerability Management (IAVM) briefings to determine whether the CSD IAM provided weekly reports to CSD Senior Management.	No relevant exceptions noted.

1.3	Corrective actions are effectively implemented.	SP5.2 Corrective actions to findings are submitted and updated by the SA and monitored by the IAM at the local level via Vulnerability Management System (VMS).	We interviewed the SMCs, ISCs, and DECC Pacific IAM to determine whether sites submitted, updated, and monitored corrective actions through VMS.	No relevant exceptions noted.
		SP5.2 Corrective actions to findings are monitored by the DAA and Certifying Authority at the headquarters level via the Vulnerability Management System (VMS).	We obtained from the DAA and Certifying Authority a description of the reports and process that the DAA and Certifying Authority used to monitor findings and corrective actions through VMS.	No relevant exceptions noted.

Risk Assessment

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
2	**Controls provide reasonable assurance that risks are periodically assessed and appropriate steps are taken to mitigate risks.**			
2.1	Risk assessments are performed according to current Federal and DOD requirements.	SP5.2 Risk assessments are performed annually IAW DODI 5200.40 or Interim DIACAP.	We obtained and reviewed the risk assessments for the SMCs, ISCs, and DECC Pacific. We determined whether the risk assessments were completed in accordance with DOD Instruction 5200.4 or Interim DIACAP.	Of the SMCs, ISCs and DECC Pacific, one ISC did not have a signed risk assessment.
		SP5.2 Risk mitigation is documented in the risk assessment.	We obtained and reviewed the most current risk assessments that the CSD IAM prepared for the SMCs, ISCs, and DECC Pacific. We verified whether the activities adequately addressed risk mitigation in their risk assessments.	The risk assessment did not adequately address risk mitigation for the three SMCs, two ISCs, and DECC Pacific.
		SP5.2 Enterprise risk assessments are prepared based on the site risk assessment results.	We requested the enterprise risk assessment.	CS did not prepare an enterprise risk assessment.

Security Plans

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
3	**Controls provide reasonable assurance that site security plans are in place, prepared, documented, and approved in accordance with Federal and DoD requirements, and is current.**			
3.1	Site security plans are documented.	SP2.1 Updates (as required) are located at the sites.	We obtained the most recent site security plans from the SMCs, ISCs, and DECC Pacific.	No relevant exceptions noted.
		SP2.1 The security plan is documented and addresses topics prescribed in OMB Circular A-130 and is on file at the DAA.	We obtained the most recent security plans from the SMCs, ISCs, and DECC Pacific. We reviewed the site security plans to determine whether topics prescribed in OMB Circular A-130 were adequately addressed. We obtained the most recent SSAA packets from the DAA to determine whether these were the same security plans we obtained from the SMCs, ISCs, and DECC Pacific.	One SMC did not adequately address the topics prescribed in OMB Circular A-130. The DAA did not have one SMC security plan on file.
3.2	Site security plans are approved.	SP2.1 The security plan for all sites is signed by the senior official on site.	We obtained the most recent site security plans from the SMCs, ISCs, and DECC Pacific to determine whether the senior site official approved the security plan.	No relevant exceptions noted.
3.3	Site security plans are current.	SP2.2 The security plan is reviewed annually and is updated as required.	We interviewed the CSD IAM to understand the security plan review process. We tested whether a security plan for each site was included with the SSAA and included on file at the DAA.	No relevant exceptions noted.

			We obtained and reviewed the most recent security plan maintained at SMCs, ISCs, and DECC Pacific. We determined whether the security plans we obtained from the DAA were the same security plans maintained at SMCs, ISCs, and DECC Pacific.	

Security Management

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
4	**Controls provide reasonable assurance that a security management structure is established and security responsibilities are clearly assigned.** **Design Weakness:** (a) DISA Computing Services did not have control procedures in place to ensure that security responsibilities are clearly assigned at all levels. Specifically, control procedures are needed to ensure the DISA Computing Services Enterprise Security Roles and Responsibilities Concept of Operations defines the responsibilities of security officials at all levels in CSD. (b) DISA did not have control procedures in place to ensure security awareness training completion is recorded and maintained in the Defense On-Line Training System (DOTS). Specifically, security awareness training encompasses two types of training-Traditional and Information Assurance Awareness, however, records for all types of training are not recorded in DOTS.			
4.1	A security management structure has been established.	SP3.1 The CSD Security Management CONOPS defines the responsibilities of security officials at all levels in CSD.	We inspected the DISA Computing Services Enterprise Security Roles and Responsibilities Concept of Operations to determine whether it defined the responsibilities of security officials for all levels in CSD.	Refer above to item (a) of the design weakness. DISA CS Enterprise Security Roles and Responsibilities Concept of Operations did not define the SMC, ISC, and DECC Pacific IAO responsibilities.

4.2	Information security responsibilities are clearly assigned.	SP3.2 The roles and responsibilities are outlined in the CSD Security management CONOPS. The IAM, IAO, and SM are assigned in their appointment orders.	We reviewed the universe of 153 IAM, IAO, and SM appointment orders obtained from the SMCs, ISCs, and DECC Pacific to determine whether the roles and responsibilities outlined in the DISA Computing Services Enterprise Security Roles and Responsibilities Concept of Operations were assigned in the appointment orders.	Refer above to item (a) of the design weakness. Of 13 SM appointment orders, 9 were not complete at three SMCs, two ISCs, and DECC Pacific. Of 13 IAM appointment orders, 12 were not complete at three SMCs, three ISCs, and DECC Pacific Of 127 IAO appointment orders, 127 did not have defined roles and responsibilities at four SMCs, three ISCs, and DECC Pacific.
4.3	CS personnel are aware of security policies.	SP3.3 Refresher security awareness training completion is recorded and maintained in DOTS.	We inspected a sample of 385 DISA personnel refresher information-assurance awareness training records from SMCs, ISCs, DECC Pacific, MPS, and CIO to determine whether DISA recorded and maintained training records in DOTS.	Refer above to item (b) of the design weakness. Of 385 DISA personnel, 182 did not have information-assurance awareness training records in DOTS at three SMCs, two ISCs, MPS, and CIO. Two SMCs and one ISC did not record and maintain information-assurance awareness training completion in DOTS.
		SP3.3 CS personnel are required to take initial security awareness training before gaining access to any system.	We inspected a sample of 344 CS personnel DD Forms 2875 at the SMCs, ISCs, and DECC Pacific to determine whether personnel took initial information assurance awareness training before gaining access to any system.	Of 344 CS personnel DD Forms 2875, 5 did not have the information assurance section completed at three SMCs and one ISC.

		SP3.3 CS personnel are required to take annual refresher security awareness training.	We inspected a sample of 344 CS personnel information-assurance training records at the SMCs, ISCs, and DECC Pacific to determine whether personnel completed annual security awareness training.	Of 344 CS personnel information-assurance training records, one SMC and one ISC did not maintain 6 training records.

Personnel

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
5	**Controls provide reasonable assurance that effective personnel policies have been implemented.**			
5.1	Employee (Government and contractor) background investigations, hiring, transferring, and termination policies address security and are in compliance with DODI 8500.2.	SP4.1 Security requirements for contractor employees are included in the contract requirements. Personnel security compliance is monitored by CS Security Managers.	We inspected a sample of 39 contracts the Defense Information Technology Contracting Organization had issued to determine whether security requirements were included. We verified with CS Security Managers that documentation for a sample of 255 contractor employees have current and valid security clearances.	No relevant exceptions noted. Of a sample of 255 contract employees, 2 employees did not have current security clearances.
		SP4.1 Personnel security checks are conducted to determine that there exists a valid and current personnel security investigation for each Government employee at the site based on the individual's duties and tasks.	We inspected a sample of 291 security background investigations for Government employees at SMCs, ISCs, and DECC Pacific to determine whether the investigations were valid and current.	Of 291 security background investigations for Government employees, 2 were not current.
		SP4.1 Termination of contractor employees requires revoking of all access to DISA applications and systems.	We inspected documentation for a sample of 120 terminated contractor employees at the SMCs, ISCs, and DECC Pacific to determine whether each employee's system access was revoked.	No relevant exceptions noted.

		SP4.1 Government employees transferring to organizations within DISA but outside CS requires revoking of all access to CS applications and systems.	We inspected the universe of seven Government employees who had transferred to organizations within DISA but outside CS to determine whether access to the CS system was revoked.	No relevant exceptions noted.
		SP4.1 Personnel security checks are conducted to determine that a valid and current personnel security investigation has been conducted for each potential employee based on the individual's duties and tasks.	We interviewed MPS to understand how MPS conducts personnel security investigations for each potential employee based on the individual's duties and tasks. We inspected a sample of 291 Government-employee personnel security investigations to determine whether they were current and valid and were based on the individual's duties and tasks.	Of 291 Government employees, 2 did not have a current personnel security investigation.
		SP4.1 Termination of Government employees requires debriefing and revoking of all access to DISA applications and systems. Termination debriefing (DISA Form 553) must be signed and maintained by the site Security Manager.	We inspected DISA Form 553 for a sample of 33 Government employees at the SMCs, ISCs, and DECC Pacific to determine whether a signed debriefing (DISA Form 553) was on file. We inspected documentation for a sample of 33 Government employees at the SMCs, ISCs, and DECC Pacific to determine whether termination included debriefing and revoking of all access to DISA applications and systems.	Of 33 Government employees, 3 did not have a DISA Form 553 maintained. Of 33 Government employees, 1 did not have a completed DISA Form 553. Of 33 Government employees, 1 did not have an out-processing checklist maintained. Of 33 Government employees, 1 did not have a completed out-processing checklist. Of 33 Government employees, 1 did not have a Non-Disclosure statement (debriefing section) maintained. Of 33 Government employees, 1 did not have a completed Non-Disclosure statement (debriefing section).

		SP4.1 Government employees transferring to organizations outside DISA requires revoking of all access to DISA applications and systems.	We inspected a sample of 33 Government employees at SMCs, ISCs, and DECC Pacific to determine whether termination of Government employees included a debrief and revoking all access to DISA applications and systems.	Of 33 Government employees, 1 did not have an out-processing checklist maintained. Of 33 Government employees, 1 did not have a completed out-processing checklist.
		SP4.1 The CS Security Handbook prescribes guidelines addressing position sensitivity designations for military and civilian employees.	We inspected the CS Security Handbook to determine whether it addressed position sensitivity for military and civilian employees.	No relevant exceptions noted.
5.2	Job descriptions for employees (Government and contractor) have been documented and employees understand their duties and responsibilities.	SD1.2 All civilian positions have position descriptions.	We inspected a sample of 287 personnel files for civilian positions from SMCs, ISCs, and DECC Pacific to determine whether the position descriptions existed.	No relevant exceptions noted.
		SD1.2 All contractor job requirements are documented within the applicable contract.	We inspected a sample of 39 contracts the Defense Information Technology Contracting Organization issued to determine whether the documented contractor job requirements were included in the contracts.	No relevant exceptions noted.
		SD1.3 Supervisors at all levels develop and maintain a performance plan (Form 208) for each individual and ensure that the plan requires the performance based on the position description.	We inspected a sample of 287 employee performance plans at the SMCs, ISCs, and DECC Pacific to determine whether the plans reflected the relevant position description.	No relevant exceptions noted.

		SD1.3 Supervisors have access to position descriptions, which identify the task and functions required by the position.	We interviewed supervisors for a sample of 226 employees at the SMCs, ISCs, and DECC Pacific to determine whether they were aware of the tasks and functions required of the employees. We compared their answers to the relevant position descriptions for appropriateness.	No relevant exceptions noted.
		SD2.1 CS management complies with DISAI 220-15-55 to ensure compliance with job descriptions and duties.	We identified personnel requirements in DISAI 220-15-55 and inspected a sample of 287 employees performance plans to determine whether the sites complied with DISAI 220-15-55.	Of 287 employees, 4 did not have mid-year reviews on their DISA Form 208 Performance Plan.
		SD3.1 Local written instructions may be followed for the performance of work.	We interviewed supervisors on work performance for a sample of 226 Government employees at the SMCs, ISCs, and DECC Pacific to determine whether work performance complied with DISAI 220-15-55.	No relevant exceptions noted.
5.3	Employees (Government and contractor) are adequately trained and possess the required skills.	SP4.2 SA certification requirements are tracked by MPS.	We inspected SA certification documentation the sites tracked for a sample of 285 SAs at SMCs, ISCs, and DECC Pacific to determine the appropriateness and completeness of site data.	Of 285 SAs, 1 did not have the SA certification signed. Of 285 SA certifications, 1 was out of the 18-month recertification scope. Of 285 SAs, 4 did not complete the final SA certification test.
		SP4.2 Training requirements for IAM and users are established by DoD and DISA policies.	We interviewed MPS staff to determine whether DoD and DISA established training requirements for IAM and users in their policies.	No relevant exceptions noted.
		SP4.2 Completion of annual Information Awareness Training is tracked by MPS and CSD IAM.	We interviewed MPS staff and CSD IAM to determine the process for tracking annual Information Awareness Training.	No relevant exceptions noted.

		SP4.2 SA certification requirements are established by DISA policies and maintained by the CIO.	We interviewed CIO staff for DoD and DISA policies used to establish SA certification requirements.	No relevant exceptions noted.
5.4	Confidentiality or Non-Disclosures agreements are documented.	SP4.1 A Non-Disclosure statement (SF 312) is required for all Government employees.	We inspected a sample of 247 Non-Disclosure statements for Government employees at the SMCs, ISCs, and DECC Pacific to determine whether employees signed the statements.	Of 247 Government employees, 2 did not sign the Non-Disclosure statement. Of 247 Government employees, 3 did not have a Non-Disclosure statement on file.
		SP4.1 A Non-Disclosure statement (SF 312) is required for all contractors.	We inspected a sample of 255 Non-Disclosure statements for contractor employees at the SMCs, ISCs, and DECC Pacific to determine whether employees signed the statements.	Of 255 contractor employees, 1 had an incomplete Non-Disclosure statement at one SMC.
5.5	Incompatible duties have been identified and policies implemented to segregate these duties.	SD1.1 Service Level Agreements also describe the roles and responsibilities of CS in maintaining the customer platforms.	We obtained and reviewed the CSD Basic Service Level Agreement to determine whether CS roles and responsibilities for maintaining customer platforms were included.	No relevant exceptions noted.
		SD1.1 CS Security Handbook describes the segregation of duties of CS security personnel. CSD OPS Policy 06-15 describes the segregation of duties of CS personnel not outlined in the CS Security Handbook.	We inspected the CSD Operations Policy Letter CSD 06-15, "Segregation of Duties," and the CS Security Handbook for segregation of incompatible duties.	No relevant exceptions noted.

Resource Classification

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
6	**Controls provide reasonable assurance that information resources are classified according to their Mission Assurance Category (MAC) and Confidentiality Level (CL).**			
6.1	Customers have communicated the classification of their applications to CS.	AC1.2 CS customers communicate Mission Assurance Criticality (MAC) levels to CS for their applications during the initial business proposal and captured in the Service Requirements Form (SRF).	We analyzed FY 2007 and FY 2008 SLAs to determine whether they : • were approved and signed by both CSD and Customer Representative, • identified the MAC and sensitivity level, and • identified how disposition of data should be handled.	No relevant exceptions noted.
6.2	Customer resource classifications and related criteria have been formally established.	AC1.2 In accordance with DODI 8500.2 and DODD 8500.1 system owner/customer establishes MAC level in the SLA based upon their assessment of the critical nature of their application or system.	We analyzed FY 2007 and FY 2008 SLAs to determine whether they identified the MAC and sensitivity level.	No relevant exceptions noted.
6.3	All DISA owned assets are classified according to criticality and sensitivity.	AC1.1 CS has defined the information resources criticality IAW the DODI 8500.2 and documented in the site SSAA or VMS.	We inspected the site's current SSAA. We ran an AS01 Report from the Vulnerability Management System at the SMCs, ISCs, and DECC Pacific, and we selected a sample of 40 assets that were both located at and owned by the site. We interviewed the IAM to determine how the IAM was notified of any new assets or changes in criticality of assets and how the IAM annotated the criticality.	No relevant exceptions noted.

		AC1.2 IAM has reviewed and noted the criticality of the DISA owned resources.	We inspected the site's current SSAA. We ran an AS01 Report from the Vulnerability Management System at the SMCs, ISCs, and DECC Pacific, and we selected a sample of 40 assets that were both located at and owned by the site. We interviewed the IAM to determine how the IAM was notified of any new assets or changes in criticality of assets and how the IAM annotated the criticality.	Of 40 assets, 1 did not have the correct Confidentiality Level at one ISC.
6.4	Service Level Agreement (SLA) management and the disposition of data requirements are identified.	AC2.3 SLAs are current and are available in the Knowledge Management System database.	We interviewed the site IAM, technical support personnel, or appropriate personnel on whether, and how, they received notification of new SLA requirements and whether they used the Knowledge Management System to receive new SLA requirements	No relevant exceptions noted.
		AC3.7 All requirements (if applicable) for communications secured by Type I or Type III crypto devices are documented in the applicable SLA.	We interviewed CCC personnel to determine whether CS used encryption tools. We requested from CCC a list of programs that require crypto or encryption (unclassified). We selected a sample of 10 programs and reviewed the applicable SLAs to determine whether the requirements were identified.	No relevant exceptions noted.
6.5	Logical controls over data files and software programs.	AC3.7 If required by the customer in the SLA and outlined in the Terms and Condition (T&C) document, encryption tools such as Virtual Private Network, Secure Socket Layer, Secure Shell, and Public Key Infrastructure are used IAW the current DOD STIGs where the data or the transmission of data needs to be protected.	We interviewed CCC personnel to determine whether CS used encryption tools. We requested from CCC a list of programs that require crypto or encryption (unclassified). We selected a sample of 10 programs and reviewed the applicable SLAs to determine whether the requirements were identified.	No relevant exceptions noted.

6.6	Correct use of encryption devices.	AC3.7 If required by the customer, all requirements for encryption are documented in the applicable SLA.	We interviewed CCC personnel on the use of encryption tools. We requested from CCC a list of programs that require crypto or encryption (unclassified). We selected a sample of 10 programs and reviewed the applicable SLAs to determine whether the requirements were identified.	No relevant exceptions noted.
		AC3.7 If required by the customer in the SLA, and included in the T&C document, the DOD encryption policy is applied in accordance with FIPS 140-2.	We interviewed CCC personnel on the use of encryption tools. We requested from CCC a list of programs that require crypto or encryption (unclassified). We selected a sample of 10 programs and reviewed the applicable SLAs to determine whether the requirements were identified.	No relevant exceptions noted.

Account Management

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
7	**Controls provide reasonable assurance that user account management procedures are implemented and effective.**			
7.1	DISA managed assets have identified authorized users and their authorized access rights.	AC2.1 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 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 access requested.	We inspected system-generated documentation for a sample of 10 mainframes for: • System Programmers • Security Administrators • Auditors • Production Control/Scheduling • Personnel • Operations Personnel • DASD Management Personnel • Storage Management Personnel to determine whether privileged users were identified. Based on the list of privileged users maintained by the IAM/IAO, we selected a sample of 288 privileged users and obtained their DD Forms 2875s to verify that the DD Forms 2875 were properly completed.	Of 10 mainframes tested, 6 had users who were granted access to operating data sets and/or system resources and were not identified as privileged users. Of 288 privileged-user DD Forms 2875 tested, 74 were not properly completed at four SMCs and three ISCs. Of the 288 privileged-user DD Forms 2875, 1 was not on file at one SMC.
		AC2.1 IAW DODI 8500.2 and appropriate DOD STIGs, the site IAM/IAO maintains a list of all approved privileged users (privilege user accounts created by CS SAs) for operating systems, networks, databases, and web administrators.	We used the assets tested in Control Objective 6.3 to generate a list of privileged users of those assets to determine whether all privileged users listed were located on the list of privileged users maintained by the IAM/IAO.	One ISC tested did not sufficiently track privileged users of Windows/Unix systems.

		AC2.1 The DODI 8500.2, as supplemented by CS Policy 06-05 and CSD Policy 06-12, details the process for granting access to system resources.	We reviewed and compared local policies regarding account management to DoD and CSD account management policies.	No relevant exceptions noted.
7.2	IAM/IAO and/or SA periodically review authorization lists to determine appropriateness.	AC2.1 Periodic revalidation of DISA managed systems, IAW applicable DOD STIGs and CS Policy 06-05, is conducted annually by the local IAM/IAO and/or SA to identify privileged accounts and privileged user accesses that are no longer needed. (Customer rental space excluded)	We interviewed the IAM, IAO, and SM at the SMCs, ISCs, and DECC Pacific to understand the revalidation process for privileged accounts or privileged user accesses. We inspected a sample of 243 privileged users DD Forms 2875 at three SMCs, three ISCs, and DECC Pacific to determine the frequency of revalidation and whether the revalidation process is in accordance with applicable DoD STIGs and CS Policy 06-05. We inspected revalidation evidence in a sample of 45 privileged accounts' at one SMC to determine the frequency of revalidation and whether the revalidation process is in accordance with applicable DoD STIGs and CS Policy 06-05.	Of 243 tested personnel, 4 were authorized users but were identified as privileged users at one SMC. Of 243 privileged users, 4 were not revalidated annually at one SMC. Of 243 privileged-user DD Forms 2875, 11 were not updated to indicate revalidation at one ISC. Of 45 asset sheets, 2 did not have a completed privileged account revalidation at one SMC.
7.3	Emergency and temporary access is controlled.	AC2.2 Emergency and temporary access authorizations are: • documented and maintained on file, • approved by appropriate management, • communicated to the IAM, and • terminated after a predetermined period on a case by case basis.	We inspected system-generated documentation for a sample of 10 mainframes to determine whether management controlled emergency and temporary access authorizations.. We interviewed CS personnel at the SMCs, ISCs, and DECC Pacific to determine whether emergency changes	Of 10 mainframes, 1 had a test ID in an active and not suspended state. No relevant exceptions noted.

			were made. For the one SMC that had emergency changes, we inspected a sample of two emergency and temporary user access requests to determine whether authorizations were: • documented and maintained on file, • approved by appropriate management, • securely communicated to the IAM, and • terminated after a predetermined period on a case-by-case basis.	

Physical Security

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
8	**Controls provide reasonable assurance that adequate physical controls have been implemented.**			
8.1	Perimeter (Base Level).	AC3.1 Physical safeguard procedures include: • controlled access and controlled perimeters for CS facilities located on military or GSA installations; • verification of DoD identification, such as a Common Access Card or DISA badge; • enclosed perimeter, by a fence that controls vehicle and pedestrian access, for CS facilities not located on military or GSA installation; • IAW local Base Support Agreement, if required, routine patrol and random door checks are performed by the local military, DoD, or GSA guards; and • access to the administrative areas is controlled by guard, mechanical cipher,	We observed the physical inner and outer perimeters of the CS facility at the SMCs, ISCs, and DECC Pacific to determine whether: • individuals attempting to access the CS facility were required to present valid DoD identification; • perimeter security was in place to control vehicle and pedestrian access; • access to administrative areas was controlled by a guard, mechanical cipher lock, or automated access control system; and • routine patrol and random door checks were performed by the military base, DoD, or GSA guards in accordance with applicable base support agreements.	No relevant exceptions noted.

		or automated access control system.		
8.2	Building, administration, and computer facility.	AC3.1 Computer Rooms not located at a DISA facility will follow the requirements of the hosting site.	We interviewed local security personnel to determine whether the three DISA DECCs not located at DISA facilities followed the host sites' requirements.	No relevant exceptions noted.
		AC3.1 The area of the computer facility that contains unclassified equipment/information is in compliance with the requirements outlined in DOD 5200.8 R, specifically: • Electronic Security System • Entry and Circulation Control • Barriers • Security Patrols/Designated Response Force.	We observed the computer facility areas that contained unclassified equipment to determine whether the areas complied with the requirements outlined in DoD 5200.8R, specifically by having: • an electronic security system, • entry and circulation control, • barriers, and • security patrols/designated response force.	No relevant exceptions noted.
		AC3.1 Computer facilities have at least two levels of physical security controls. • Access to the computer facility requires positive identification of the employee. Through the use of something they have (e.g., proxy card, DOD identification card, etc.), something they know (e.g., pin number, etc.) and /or something they are (e.g., biometrics) • Employees must wear their picture identification cards above the waist.	We observed access to the computer facilities for the SMCs, ISCs, and DECC Pacific to determine whether such access required at least two levels of physical security controls through the use of something they have (for example, a proxy card or DoD identification card); something they knew (for example, a personal identification number); or something they were, (for example, biometrics). We observed CS employees at the SMCs, ISCs, and DECC Pacific to	No relevant exceptions noted.

		Employees not in compliance will be challenged.	determine whether picture identification cards were worn above the waist. We observed whether security or others challenged CS employees who did not comply.	
8.3	Visitors are controlled.	AC3.1 All CS site SMs must maintain an authorized access list to the CS facility.	We inspected authorized access lists for a sample of employees at the SMCs, ISCs, and DECC Pacific to determine whether facility access was appropriate.	No relevant exceptions noted.
		AC3.1 Personnel who do not have the appropriate security investigation or clearance will be escorted at all times while in the computing facility.	We interviewed the site SM at the SMCs, ISCs, and DECC Pacific to understand the local site-specific badge color codes and the process for escorting visitors. We observed visitors with badges who required escort to determine whether such visitors were escorted at all times.	No relevant exceptions noted.
		AC3.2 Visitors to the computing facilities that are not on the authorized access list must be validated by the local security officer, and signed in and out of the facility and will be escorted as required.	We interviewed the local security officer and security guards for the SMCs, ISCs, and DECC Pacific about how they handled visitors who were not on the authorized access list. We observed security officers and visitors at the SMCs, ISCs, and DECC Pacific to determine whether local security officers validated the visitors.	No relevant exceptions noted.
8.4	Traditional Security Review.	AC3.3 As part of the site certification and accreditation process, a periodic Traditional Security review is conducted by the Certifying Authority at a minimum every 3 years or more frequently based on the classification levels processed by the site.	We interviewed FSO personnel about the system classification levels and how they affected the traditional security review process and schedule. We inspected the traditional security review schedule the FSO provided to	No relevant exceptions noted.

			determine whether the FSO performed the reviews in accordance with the system classification levels. We inspected DITSCAP documentation and the traditional security review for the SMCs, ISCs, and DECC Pacific to determine the date of the last traditional security review.	

Logical Access Controls

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
9	**Controls provide reasonable assurance that adequate logical access controls have been implemented.** **Design Weakness:** CS does not have control procedures in place to ensure that adequate logical access controls have been implemented. Specifically, control procedures are needed to ensure the following: (a) password configurations are in compliance with DoD STIGs and (b) all access paths have been identified and controls implemented to prevent and detect access.			
9.1	Passwords, tokens, or other devices are used to identify and authenticate users.	AC3.2 Password configuration requirements, at the system level, will be in compliance with appropriate current DOD STIG or JTF-GNO policy.	We inspected system-generated documentation for a sample of 10 mainframes, 34 UNIX, 56 Windows, and 42 network devices the SMCs and ISCs managed to determine whether the password configuration settings complied with the appropriate DoD STIG or JTF-GNO policy.	Refer above to item (a) of the design weakness. Password configurations were not set in accordance with the appropriate DoD STIG or JTF-GNO policy for 2 of 10 mainframes, 2 of 34 UNIX, 6 of 56 Windows, and 2 of 42 network devices tested.
		AC3.2 Vendor-supplied default logons and passwords will be removed, changed or disabled in accordance with appropriate current DOD STIG or JTF-GNO policy.	We inspected system-generated documentation for a sample of 10 mainframes, 34 UNIX, 56 Windows, and 42 network devices the SMCs and ISCs managed to determine whether the vendor-supplied default logons and	No relevant exceptions noted.

			passwords were removed, changed, or disabled in accordance with the appropriate DoD STIG or JTF-GNO policy.	
		AC3.2 Passwords are checked for compliance to current DOD STIG or JTF-GNO policy as part of DISA approved scanning tool, password cracking utilities, or SRRs.	We inspected the configuration of password cracking software for a sample of 10 mainframes, 34 UNIX, 56 Windows, and 42 network devices the SMCs and ISCs managed to determine whether management checked passwords for compliance with current DoD STIG or JTF-GNO policy.	Of 34 UNIX servers tested, 2 did not have passwords checked using an approved utility.
9.2	Sanitation of equipment and media prior to disposal or reuse.	AC3.8 Sanitation of equipment and media prior to disposal or reuse are performed in accordance with DoD Regulation 5200.1-R, CS Security Handbook, CSD Policy 06-29, CSD Policy 06-17 and the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," dated June 4, 2001.	We interviewed local security personnel to determine whether the process of disposing equipment and media that the SMCs, ISCs, and DECC Pacific followed complied with DoD and local policies. We inspected sanitized equipment logs for a sample of 88 pieces of equipment and verified evidence of proper sanitization and disposal.	No relevant exceptions noted.
9.3	Access paths have been identified and controls implemented to prevent or detect access.	AC3.4 Access paths are identified within the communications topography for each CS site. The communication topography shows connections from the wide area network into the perimeter point of presence down to the individual Internet Protocol addresses of all devices within the enclave.	We interviewed CCC personnel to ensure they identified access paths and showed the paths on network diagrams, and to ensure controls were in place to prevent or detect access. We interviewed CCC personnel to determine how and when they updated network diagrams.	No relevant exceptions noted.

		AC3.4 System software is configured in accordance with the current DOD STIG, Admin LAN CONOPS, and DISA DPL 06-10.	We inspected system-generated documentation for a sample of 10 mainframes, 34 UNIX, 56 Windows, and 42 network devices that the SMCs and ISCs managed. We determined whether the operating system software was configured in accordance with the current DoD STIG and CSD Policy.	Refer above to item (b) of the design weakness. Of the samples tested, 10 of 10 mainframes, 34 of 34 UNIX, 55 of 56 Windows, and 15 of 42 network devices were not configured in accordance with the current DoD STIG and CSD Policy.
		AC3.4 Network diagrams are developed and maintained to show access paths.	We interviewed CCC personnel to ensure they identified access paths and showed the paths on network diagrams, and to ensure controls were in place to prevent or detect access. We interviewed CCC personnel to determine how and when they updated network diagrams.	No relevant exceptions noted.
		AC3.4 Operating system software is configured IAW the current DOD STIG and CSD Policy.	We inspected system-generated documentation for a sample of 10 mainframes, 34 UNIX, 56 Windows, and 42 network devices managed by the SMCs and ISCs. We determined whether the operating system software was configured in accordance with the current DoD STIG and CSD Policy.	Refer above to item (b) of the design weakness. Of samples tested, 10 of 10 mainframes, 34 of 34 UNIX, 55 of 56 Windows, and 15 of 42 network devices were not configured in accordance with the current DoD STIG and CSD Policy.
		AC3.4 Access to data files and software programs is configured IAW the current DOD STIG and CSD Policy.	We inspected system-generated documentation for a sample of 10 mainframes, 34 UNIX, 56 Windows, and 42 network devices managed by the SMCs and ISCs to determine whether access to data files and software programs is configured in accordance with the current DoD STIG and CSD Policy.	Of samples tested, 8 of 10 mainframes, 25 of 34 UNIX, 16 of 56 Windows, and 1 network device were not in accordance with DoD STIG and CSD Policy.

Networks and Telecommunications

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
10	**Controls provide reasonable assurance that Networks and telecommunications are secure.**			
10.1	Telecommunication defense.	AC3.6 Dial-in telephone numbers are not published.	We interviewed personnel at the SMCs, ISCs, and DECC Pacific to determine who managed dial-up services, whether the services were centrally managed (permission for remote access) or at each location, and whether the telephone numbers were published.	No relevant exceptions noted.
		AC3.6 Telecommunications access is controlled by the managing CCC for the network devices, to include firewall and network IDSs, at all sites within continental United States for unclassified wide area network. CCC personnel have access to those networks through the out-of-band virtual private network tunnel for all networks so equipped.	We interviewed CCC personnel to determine how they controlled and managed the networks. We identified what controls were in place to ensure that only access to the network or production network through the out-of-band network.	No relevant exceptions noted.
10.2	Network defense.	AC3.4 Network access paths are configured to prevent circumvention of security and unauthorized access in accordance with the current DOD STIGs and CSD OPS policy.	We inspected a sample of 10 mainframes and 42 network devices to determine whether configurations complied with current DoD STIGs and CSD OPS policy.	Of 10 mainframes, 2 were not configured in accordance with DoD STIG and CSD OPS Policy.
		AC3.4 Networking equipment is configured in accordance with the current DOD STIGs and CSD OPS policy.	We inspected a sample of 42 network devices to determine whether configurations complied with current DoD STIGs and CSD OPS policy.	Of 42 network devices tested, 14 were not configured in accordance with the current DoD STIG and CSD OPS Policy.

10.3	Remote and dial-up capabilities are controlled.	AC3.4 Remote access is established in accordance with current DOD STIGs.	We interviewed personnel at the SMCs, ISCs, and DECC Pacific to determine how remote access was established. We reviewed site policies and procedures to determine whether procedures complied with DoD STIGS.	No relevant exceptions noted.
10.4	Actual or attempted unauthorized, unusual, or sensitive network access is monitored.	AC3.5 Network intrusion detection systems are installed in accordance with the DOD STIGs and monitor unusual and/or inappropriate activity.	We inspected system-generated documentation for a sample of 23 UNIX, 32 Windows, and 28 network devices managed by the CCCs to determine whether intrusion detection systems were installed in accordance with DoD STIGs.	Of samples tested, 22 of 23 UNIX and 11 of 32 Windows did not have host-based intrusion detection systems installed in accordance with the current DoD STIG.
		AC3.5 Procedures are in place for monitoring, investigating, and reporting inappropriate or unusual activity. The DOD STIG and CS Policy outlines what activity is to be monitored for inappropriate or unusual activities.	We obtained and compared the local policies from the SMCs, ISCs, and DECC Pacific to determine whether personnel complied with the CSD network monitoring policy.	No relevant exceptions noted
10.5	Suspicious network access activity is investigated and appropriate action is taken.	AC4.2 Suspicious access activity is investigated and appropriate action taken in accordance with GS4 LOI 07-11and CS Policy 06-02.	We interviewed personnel at the CCCs, SMCs, ISCs, and DECC Pacific to understand how they monitored suspicious activity. We inspected records for a sample of 104 suspicious activities reported from April 1, 2007, to month date, year, to verify that personnel followed the appropriate policies when reporting the suspicious activities.	No relevant exceptions noted.

Access Monitoring

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
11	**Controls provide reasonable assurance that access is monitored, suspected security violations are investigated, and appropriate remedial action is taken.** **Design Weakness:** CS does not have control procedures in place to ensure that access is monitored, suspected security violations are investigated, and appropriate remedial action is taken. Specifically, control procedures are needed to ensure that audit trails are being maintained and reviewed.			
11.1	Audit trails are maintained.	AC3.5 System auditing review is in accordance with DOD STIGs. (Please refer to CSD Management Letter)	We interviewed DECC personnel to determine: • how they configured audit trails to capture data and which data; • the frequency of backups, the location of the alternate media, and the retention timeframe by technology; and, • how they conducted the review of the audit trails. We interviewed SAs and IAOs for a sample of 10 mainframes, 34 UNIX, 56 Windows, and 42 network devices the SMCs and ISCs managed to determine whether the auditing review was in accordance with DoD STIGs.	Three SMCs and one ISC did not review audit logs based on DoD requirements. Of samples tested, 4 of 34 UNIX and 2 of 56 Windows systems did not have evidence that confirmed personnel reviewed audit trails and system log files in accordance with DoD STIGs.
		AC3.5 System auditing is enabled in accordance with DOD STIGs. (Please refer to CSD Management Letter)	We interviewed SAs and IAOs for a sample of 10 mainframes, 34 UNIX, 56 Windows, and 42 network devices the SMCs and ISCs managed to determine whether system auditing was	Refer to the design weakness above. Of samples tested, 7 of 10 mainframes, 4 of 34 UNIX, and 2 of 56 Windows servers were not configured to audit in accordance with DoD STIGs.

			enabled in accordance with DoD STIGs.	
		AC4.1 Auditing is conducted in accordance with DOD STIGs. (Please refer to CSD Management Letter)	We interviewed SAs and IAOs for a sample of 10 mainframes, 34 UNIX, 56 Windows, and 42 network devices the SMCs and ISCs managed to determine whether an audit was conducted in accordance with DoD STIGs.	Of 10 mainframes, 7 did not have auditing conducted in accordance with DoD STIGs. Of samples tested, 4 of 34 UNIX, 10 o f 56 Windows, and 13 of 42 network devices did not retain audit logs in accordance with DoD STIGs. Of 56 Windows servers, 1 did not back up audit records to a separate media.
11.2	Effective incident response capability has been implemented.	SP3.4 TMS Remedy Tickets and/or email is used as CSD's incident response and reporting tool. Specifically, the following items from the questionnaire must be completed: • Were redundant systems available and working? If no, explain. • Confirm the overall impact the outage has on the customer mission. • Was scheduled batch processing jobs delayed? If yes, ensure question (2) is completely answered. • How many customer/user calls have been received? • Does this Incident exist in the Known Error Database (KEDB)?	We interviewed personnel at the SMCs, ISCs, and DECC Pacific to determine how they performed incident response and reporting. We inspected a sample of 247 TMS tickets at the SMCs, ISCs, and DECC Pacific to determine whether personnel properly completed the questionnaires.	Of 247 TMS tickets, 15 had incorrect, incomplete, or missing questionnaires at two SMCs and two ISCs.
		SP3.4 GS4 07-11 and CS Policy Letter CSD 06-02 provides guidance on handling incidents, incident reporting structure, and prioritization of incidents that are consistent with attributes noted in DODI 8500.2	We determined whether the SMCs, ISCs, and DECC Pacific followed the CSD Incident Handling Plan or local Incident Handling Plan. We determined whether the CSD Incident Handling Plan (GS4 07-11 and CS Policy Letter CSD 06-02) or the local plan complied with DoD policy.	No relevant exceptions noted.

Change Control

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
12	**Controls provide reasonable assurance that changes to DISA owned assets are properly controlled.**			
12.1	DISA initiated specific software or hardware modifications are authorized and the documentation is maintained.	CC1.1 Customer requested changes: In accordance with CS Operational Change and Configuration Management Plan, proposed changes to hardware, operating system, utility software, communications, and networks are reviewed and approved in accordance with established criteria. Local Change Control Boards (CCBs) are in place at each of the four SMCs and three ISCs to oversee the change review and approval process. The site IAM is a voting member of the local CCBs.	At the SMCs, ISCs, and DECC Pacific, we: • obtained the local CCB charter; • sought to understand the local CCB process, and we documented that process; • obtained a list of the local CCB members and asked whether the site IAM was a voting member of the CCB • obtained copies of the minutes for the last five CCB meetings. We reviewed and determined whether the minutes contained discussions of approval and disapproval of changes to hardware and OS software; and, • asked how distribution and implementation of software was communicated to appropriate organizations, and asked whether there was an audit trail of software distribution. At two SMCs and one ISC, we asked whether the site used Software Factory (SWF) or another system to track software distribution.	No relevant exceptions noted.

		CC1.1 In accordance with CS Operational Change and Configuration Management Plan, proposed changes to hardware, operating system, utility software, communications, and networks are reviewed and approved in accordance with established criteria. Local CCBs are in place at each of the four SMCs and three ISCs to oversee the change review and approval process. The site IAM is a voting member of the local CCBs.	At the SMCs, ISCs, and DECC Pacific, we: • obtained the local CCB charter; • sought to understand the local CCB process, and we documented that process; • obtained a list of the local CCB members and asked whether the site IAM was a voting member of the CCB; • obtained copies of the minutes for the last five CCB meetings. We reviewed and determined whether they contained discussions of approval and disapproval of changes to hardware and OS software; • inquired how distribution and implementation of software was communicated to appropriate organizations, and whether there was an audit trail of software distribution. At two SMCs and one ISC, we asked whether the site used Software Factory (SWF) or another system to track software distribution.	No relevant exceptions noted.
		CC3.2 Verification and acceptance of OS and utility software changes is documented and approved, and movements are controlled. The ESCCB provides this control for OS and utility software at the Corporate level. Local Change Management controls the implementation of OS and executive software changes at the SMC and ISC level. All ESCCB actions are documented and approved. Minutes of each ESCCB meeting are published and	We inspected the ESCCB operating procedure document outlining the role of the ESCCB to determine whether the ESCCB controlled utility and operating system changes. We inspected evidence to determine whether the ESCCB documented and approved all ESCCB actions, and whether the minutes of the ESCCB meetings were available.	No relevant exceptions noted.

		all documentation is maintained and is available online or upon request. The actual distribution IBM mainframe software is controlled via an ESCCB and Software Factory (SWF) interface. All software distributed by the SWF is tracked, notifications are provided to appropriate organizations and a complete audit trail is retained.	We inspected the System Support Office product procedure installation guide for the mainframe systems at one site to determine whether the System Support Office tracked, notified all appropriate organizations, and retained a complete audit trail for all software distributed by the SWF.	
12.2	New and modified hardware and OS/utility software is tested and controlled according to specific criteria.	CC2.1 As part of the SSOPAC process for IBM mainframe OS releases: • integration testing is performed to ensure functionality; • performance and stress testing is performed, as required, to identify impacts on system performance; • security testing is performed for each OS system software release. Based upon test results, actions are initiated to rectify identified software deficiencies, performance impacts, and security problems.	We interviewed System Support Office management personnel for the IBM mainframes based at DECC Mechanicsburg to determine their process for performing integration tasking, performance and stress testing, and security testing on IBM mainframe operating system releases	No relevant exceptions noted.
		CC2.1 Document changes to hardware and OS software in the minutes of the CCB.	At the SMCs, ISCs, and DECC Pacific, we: • obtained the local CCB charter; • obtained an understanding of the local CCB process and documented that process; • obtained a list of the local CCB members and inquired whether the site IAM is a voting member of the CCB; • obtained copies of the last five CCB meeting minutes. Reviewed and determined whether they contain discussions of approval and disapproval of changes to hardware and OS	No relevant exceptions noted.

			software; and • inquired how distribution and implementation of software was communicated to appropriate organizations, and whether there was an audit trail of software distribution.	
		CC2.1 New systems, and changes to existing systems, are reviewed by an approving authority prior to connection to the network in accordance with CSD Policy Letter GS4 07-16.	We inspected documentation for a sample of 302 Category I and II Changes to ensure they complied with CS Standard Operating Procedure 07-16.	No relevant exceptions noted.
12.3	Emergency changes are promptly approved.	CC2.2 Emergency change procedures are documented in the CS Change and Configuration Management Plan.	We reviewed the DISA CS Operational Change and Configuration Management Plan to ensure it complied with DoD Instruction 8500.2.	No relevant exceptions noted.
12.4	Movement of programs and data among libraries is controlled.	CC3.1 Mainframe Executive Software products are recorded and tracked. Inventories are maintained which include version, maintenance level, out-of-support date, and documentation.	We inspected system documentation from the Mechanicsburg SWF for mainframe systems to determine whether mainframe executive software programs were recorded and tracked, and whether an inventory was maintained that included the version, maintenance level, out-of-support date, and related documentation	No relevant exceptions noted.
12.5	Use of public domain and personal software is restricted.	CC1.2 Use of personal and public domain software on Government Equipment is in accordance with DODD 8500.1 and CSD OPS policy 06-03.	We inspected a sample of 80 desktop computers to verify personal and public domain software was in accordance with DOD Instruction 8500.1 and CSD OPS Policy 06-03.	Of 80 desktop computers, 9 contained unauthorized software at two SMCs and one ISC.

Service Continuity

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
13	**Controls provide reasonable assurance that procedures and controls are in place to prevent or minimize unexpected interruptions.**			
13.1	Data and program backup procedures have been implemented.	SC2.1 As a standard service, each site has an off-site and transportation agreement. (The customer must agree to pay for additional services not included in the standard package and documented in the SLA.)	We interviewed computer center operations staff at the SMCs, ISCs, and DECC Pacific to determine their off-site and transportation requirements for backup media. We inspected the off-site transportation agreement for the SMCs, ISCs, and DECC Pacific to determine whether personnel transported backup media to the off-site location in accordance with SLA requirements.	No relevant exceptions noted.
		SC2.1 Standard data and program backup procedures (outlined in CS Policy Ltr 06-01) are conducted in accordance with the appropriate DOD STIGs, SLA requirements and CSD Policy Ltr 06-01. (The customer must agree to pay for additional services not included in the standard package and documented in the SLA.)	We inspected the off-site transportation agreement for SMCs, ISCs, and DECC Pacific to determine whether the agreement included: • weekly full data backup, • incremental daily backup, • detailed back up procedures, • a plan for rotating backup media, and • storage and retention procedures for backup media.	No relevant exceptions noted.

13.2	Environmental Controls have been implemented.	SC2.2 Computing facilities and support areas have automatic notification of activation of smoke detectors that alarm locally and at supporting fire department. • Some administration areas have automatic notification of activation of smoke detectors. Some of these alarm locally; some alarm locally and at the supporting fire department. • Fire inspections are made based on local site rules. • Computing facilities and support areas have automatic activation of fire suppression systems. • Administration areas have either automatic activation of fire suppression systems or hand-held extinguishers located throughout the area.	At the SMCs, ISCs, and DECC Pacific, we interviewed data center personnel and inspected the data center to determine whether the following environmental controls were in place: • automatic notification of activation of smoke detectors that alarms locally and at the supporting fire department, • annual fire inspections, • automatic activation of fire suppression systems, and • administration areas either having automatic activation of fire suppression systems or hand-held extinguishers.	No relevant exceptions noted.
		SC2.2 Computer facilities have: • automatic humidity and temperature controls systems that 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 alarm if the voltage fluctuates beyond established safe operations levels; • a minimum of two electrical feeds; • battery powered uninterrupted power system to provide sufficient power to all systems in the computer room to allow for at least 20 minutes of operations • backup generators that are set to	At the SMCs, ISCs, and DECC Pacific, we interviewed data center personnel and inspected the data center to determine whether the following environmental controls were in place: • automatic humidity and temperature controls systems that alarm; • a master power switch located at or near the main entrance, labeled and protected by a cover to prevent accidental shut-off; • automatic voltage control systems that alarm; • a minimum of two electrical feeds; • battery powered uninterrupted power supplies and voltage regulators; and • backup generators that are tested monthly and set to automatically start.	Temperature and humidity gauges were not working properly at one ISC.

		automatically start-up and generate power when commercial power fails. The generators are tested monthly for operations and power generations. Additional fuel and spare parts are on hand to provide for sustained operations.		
13.3	IT Hardware maintenance controls have been implemented.	SC2.4 Policies and procedures for IT equipment maintenance exist and are up-to-date.	We reviewed IT equipment maintenance policies and procedures to determine their adequacy for the current operating environment of the computing facility.	No relevant exceptions noted.
		SC2.4 Routine periodic preventive maintenance on IT equipment is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations or as provided for in the maintenance contract.	We interviewed computer operations personnel at the SMCs, ISCs, and DECC Pacific to determine the process for scheduling preventative maintenance on facilities equipment and tracking completion of scheduled maintenance.	No relevant exceptions noted.
		SC2.4 Regular and unscheduled maintenance on IT equipment is performed and documented.	We interviewed computer operations personnel at the SMCs, ISCs, and DECC Pacific to determine the process for scheduling maintenance on IT equipment and documenting completion of scheduled/unscheduled maintenance.	No relevant exceptions noted.
		SC2.4 Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintenance.	We obtained and reviewed the schedule for routine IT equipment preventive maintenance. We interviewed the Facilities Manager to determine whether personnel documented the unscheduled maintenance on IT hardware.	No relevant exceptions noted.

			We requested any unscheduled maintenance records that occurred in the previous 6 months.	
		SC2.4 Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	We interviewed computer operations personnel for the SMCs, ISCs, and DECC Pacific to determine whether spare or backup hardware inventory existed.	No relevant exceptions noted.
		SC2.4 Records are maintained on the actual performance in meeting IT equipment service schedules.	We obtained and reviewed the schedule for routine IT equipment preventive maintenance. We obtained and reviewed the IT hardware maintenance records. We compared the maintenance records to the maintenance service schedule and determined whether the records were in accordance to the service schedule.	No relevant exceptions noted.
13.4	Staff have been trained to respond to emergencies.	SC2.3 Data center staff receive periodic training in emergency fire, flooding, and alarm incident procedures.	We interviewed the Security Manager to determine whether employees received initial and annual training in emergency response. We determined how the site keeps track of employees' understanding and training of emergency response procedures.	No relevant exceptions noted.
		SC2.3 Emergency response procedures are documented.	We inspected emergency response procedures for the SMCs, ISCs, and DECC Pacific to determine whether procedures were documented.	No relevant exceptions noted.

		SC2.3 Emergency procedures are periodically tested.	We inspected emergency plans and test results for the SMCs, ISCs, and DECC Pacific to determine whether personnel tested emergency procedures annually and documented the test results.	One ISC did not perform an annual fire drill.
		SC2.3 Data center employees have received training and understand their emergency roles and responsibilities.	We interviewed the SM at the SMCs, ISCs, and DECC Pacific to determine whether employees received initial and annual training in emergency response. We determined how the site tracked employees' understanding and training of emergency response procedures.	No relevant exceptions noted.
13.5	Facility maintenance controls have been implemented.	SC2.4 Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintenance.	We interviewed the Facilities Manager at the SMCs, ISCs, and DECC Pacific to determine whether there was backup facilities equipment to accommodate scheduled/unscheduled maintenance. We interviewed the Facilities Manager to determine who performed the scheduled/unscheduled maintenance. We verified with the Base Support Agreement/Interagency Support Agreement to determine whether authorized personnel performed maintenance.	No relevant exceptions noted.

		SC2.4 Records are maintained on the actual performance in meeting facilities equipment service schedules.	We obtained and reviewed the schedule for routine facility equipment preventive maintenance. We obtained and reviewed the facilities maintenance records (for example, records for generator/fuel tanks, batteries/Uninterrupted Power Supply, and chillers). We compared the maintenance records to the maintenance service schedule obtained and determined whether the records were in accordance to the service schedule.	No relevant exceptions noted.
		SC2.4 Regular and unscheduled maintenance on facilities equipment is performed and is documented.	We interviewed the Facilities Manager at the SMCs, ISCs, and DECC Pacific and determined whether personnel documented regular/unscheduled maintenance on facility equipment. We obtained and reviewed the facilities maintenance records (for example, records for generator/fuel tanks, batteries/UPS, and chillers). We requested any unscheduled maintenance records that occurred within the previous 6 months.	No relevant exceptions noted.
		SC2.4 Routine periodic preventive maintenance on facilities equipment is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.	We interviewed the Facilities Manager at the SMCs, ISCs, and DECC Pacific to determine who performed routine periodic preventive maintenance on facilities equipment and whether authorized persons performed maintenance in accordance with the Base Support Agreement/Interagency Support Agreement.	No relevant exceptions noted.

Section IV: Supplemental Information Provided by DISA

The DISA 2005 Statement on Auditing Standards No. 70 project included some conditions pertaining to security systems and procedures that are beyond the purview of CS. The following is a summary of those issues that continue to require support from external sources and were identified prior to inception of the 2006 project.

2005 Results of Testing Requiring DoD or DISA Enterprise Solutions

Audit Trails. The DoD Office of Inspector General recommended that the CS Director implement more consistent procedures across the enterprise to create, monitor and review, protect, and maintain CS system audit trails in order to comply with the requirements of DoD Instruction 8500.2 and STIGs. In addition, it was recommended that CS implement and configure software audit capabilities such that security personnel could extract critical events from system data on a daily basis; conduct in-depth, daily reviews of all audit trails for suspicious activity; and investigate security incidents with automated access to all audit data.

Status: DISA does not currently have the automated tools required to meet these objectives. Implementation of the appropriate programs is pending implementation resources and technical recommendations from the DISA FSO.

Host-Based Intrusion Detection Systems. It was recommended that the CS Director deploy host-based intrusion detection systems software on all major application servers, network management assets, and domain name servers, in accordance with DoD Instruction 8500.2 and the STIGs.

Status: DoD has awarded a contract for an enterprise-wide, host-based security solution. CS is implementing the DoD-wide, host-based security solution.

Scope

Defense Enterprise Computing Centers in Scope of This Report

Systems Management Centers
- Mechanicsburg, Pennsylvania
- Montgomery, Alabama
- Ogden, Utah
- Oklahoma City, Oklahoma

Infrastructure Services Centers
- Columbus, Ohio
- San Antonio, Texas
- St. Louis, Missouri

Pacific, Pearl Harbor, Hawaii

Acronyms and Abbreviations

BMC	Business Management Center
CCC	Communications Control Center
CIO	Chief Information Officer
CS	Center for Computing Services
DAA	Designated Approving Authority
DECC	Defense Enterprise Computing Center
DISA	Defense Information System Agency
DITSCAP	Defense Information Technology Certification and Accreditation Process
DoD	Department of Defense
FSO	Field Security Operations
GIG	Global Information Grid
GSA	General Services Administration
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAR	Information Assurance Review
IDS	Intrusion Detection System
ISC	Infrastructure Services Center
IT	Information Technology
MAC	Mission Assurance Category
MPS	Manpower, Personnel, and Security
OMB	Office of Management and Budget
PE	Processing Element
POA&M	Plan of Action and Milestones
SA	System Administrator
SLA	Service-Level Agreement
SM	Security Manager
SMC	System Management Center
SRR	Security Readiness Review
SSAA	System Security Authorization Agreement
SSO	System Support Office
STIG	Security Technical Implementation Guide
VMS	Vulnerability Management System

Report Distribution

Office of the Secretary of Defense

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

Department of the Army

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

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Combatant Commands

Commander, U.S. Joint Forces Command
    Inspector General, U.S. Joint Forces Command
Commander, U.S. Strategic Command

Other Defense Organizations

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

Non-Defense Federal Organization

Office of Management and Budget
Government Accountability Office

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Finance, and Accountability, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform

Team Members

The Department of Defense Office of the Deputy Inspector General for Auditing, Defense Financial Auditing Service, in conjunction with contract auditors from Ernst & Young LLP, prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Patricia A. Marsh
Patricia C. Remington
Richard Ng
G. Marshall Grimes
Suzette L. Luecke
Chi H. Lam
Tomasa Pack
Patricia Joyner
Wen-Tswan Chen
Jenny R. Ansel
Catherine Cervantes
Kenneth J. Bensman
Justin L. Symonds
Robert Shell
Kandasamy Selvavel
Eric Bisignano
Anh Tran
Edward Kell
Jaime A. Bobbio
Minh Q. Tran
Patricia Papas
Erin S. Hart

Inspector General
Department of Defense