November 15, 2006

Information Technology Management

Defense Information Systems Agency Controls of the Center for Computing Services Placed in Operation and Tests of Operating Effectiveness for the Period December 1, 2005, through July 31, 2006

(D-2007-022)

Department of Defense
Office of Inspector General

Quality *Integrity* *Accountability*

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 NOV 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Technology Management: Defense Information Systems Agency Controls of the Center for Computing Services Placed in Operation and Tests of Operating Effectiveness for the Period December 1, 2005, through July 31, 2006	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **ODIG-AUD (ATTN: Audit Suggestions),Department of Defense Inspector General,400 Army Navy Drive (Room 801),Arlington,VA,22202-4704**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**79**	

Additional Copies

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

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Office of the Deputy Inspector General for Auditing at (703) 604-8940 (DSN 664-8940) 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

November 15, 2006

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

SUBJECT: Report on Defense Information Systems Agency Controls of the Center for Computing Services Placed in Operation and Tests of Operating Effectiveness for the Period December 1, 2005, through July 31, 2006 (Report No. D-2007-022)

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. Questions should be directed to Ms. Patricia C. Remington at (703) 428-1054 (DSN 328-1054) or Ms. Suzette L. Luecke at (703) 428-1067 (DSN 328-1067). The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

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

Table of Contents

FOREWORD

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

The DoD Office of Inspector General is implementing a long-range strategy to conduct audits of DoD financial statements. The Chief Financial Officers Act of 1990, as amended, mandates that agencies prepare and conduct audits of financial statements. The reliability of information processed at the DISA sites directly impacts 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 both 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 controls defined by DISA over the CS environment. The report provides an opinion on the fairness of presentation by DISA 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 were previously performed by user organizations to plan or conduct financial statement and performance audits. This examination will also provide a separate audit report with recommendations to management for correction of identified internal control deficiencies.

Effective internal control is a critical and required element necessary 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 compliance by DISA 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

November 15, 2006

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

SUBJECT: Report on Defense Information Systems Agency Controls of the Center for Computing Services Placed in Operation and Tests of Operating Effectiveness for the Period December 1, 2005, through July 31, 2006 (Report No. D-2007-022)

We have examined the accompanying description of information technology controls of the Defense Information Systems Agency (DISA) over selected Defense Enterprise Computing Centers (DECCs) managed by the Center for Computing Services (CS). We examined controls related to unclassified technologies (operating systems) at selected DECCs, listed in the Scope appendix on page 65. 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 July 31, 2006. 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 information resources criticality and sensitivity were known and properly documented within the service-level agreements. These deficiencies resulted in controls not being suitably designed to achieve Control Objective 6, "Controls provide reasonable assurance that information resources are classified according to their criticality and sensitivity."

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 12, "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 July 31, 2006. 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 December 1, 2005, to July 31, 2006. 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.

As discussed in the accompanying description of controls and in our description of the tests of operating effectiveness, CS has controls in place to document reportable computer operations incidents in accordance with DISA CS Instruction 360-225-1, ”Event Reporting,” December 7, 2004. Our tests of operating effectiveness, however, indicated that not all such incidents are being documented in accordance with the Instruction. This resulted in the non-achievement of Control Objective 11, “Controls provide reasonable assurance that an effective incident response capability has been implemented.”

In our opinion, except for the deficiency in operating effectiveness and the non-achievement of the related control objective noted in the previous paragraph, 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 December 1, 2005, to July 31, 2006.

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 July 31, 2006, and information about tests of the operating effectiveness of specific controls covers the period from December 1, 2005, to July 31, 2006. 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
for Paul J. Granetto, CPA
Assistant Inspector General and Director
Defense Financial Auditing Service

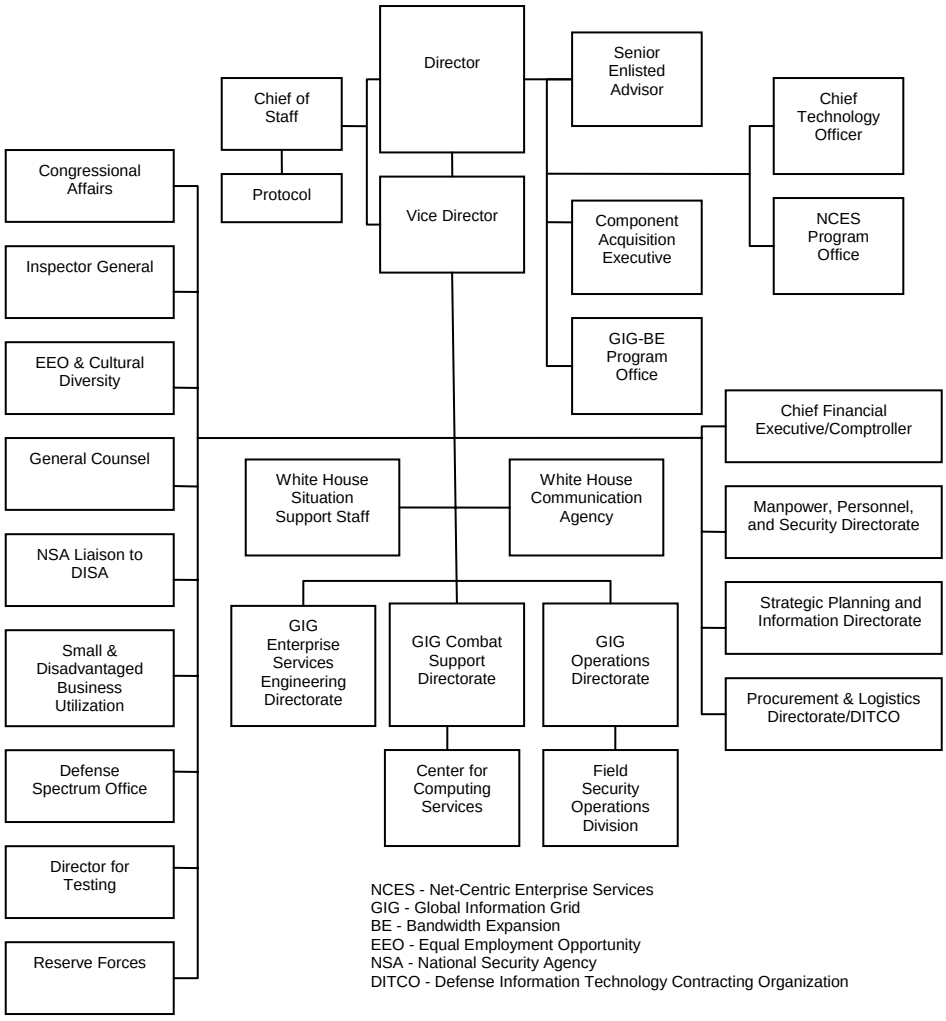
Section II: Information Provided by DISA

Overview of Operations

Defense Information Systems Agency

The Defense Information Systems Agency (DISA) is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components, under all conditions of peace and war. DISA is the provider of global net-centric[1] solutions for the nation's war fighters and all those who support them in the defense of the Nation. The core services are Acquisition, Center for Computing Services (CS), Enterprise Services, Network Operations, Network Services, Net-Centric Enterprise Services, and Global Information Grid (GIG)-Bandwidth Expansion. Chart 1 provides the organizational structure of DISA.

Chart 1. Defense Information Systems Agency



[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.

This report focuses on the controls over CS, which is under the GIG Combat Support Directorate. This report addresses controls that are owned by other DISA organizations like the CIO office and FSO, under the GIG Operations Directorate, as they relate to CS operations and general controls over the Defense Enterprise Computing Centers (DECCs).

Center for Computing Services

The CS provides computer processing for the entire gamut of combat support functions, including transportation, logistics, maintenance, munitions, engineering, acquisition, finance, medicine, and military personnel readiness. With more than 800,000 users, CS operates over 1,400 applications in 18 geographically separate facilities using more than 40 mainframes and 3,000 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.

CS features diverse locations, a Defense-in-depth philosophy, and dual high-capacity Defense Information System Network connectivity. CS also uses automated systems management to control computing resources and realize economies of scale. CS has adopted assured computing philosophies and 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 through utility contracts, enables DISA to provide the availability and surge capabilities that customers require.

CS offers computing services on both DISA- 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; Stuttgart, 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 2 provides the organizational structure of CS.

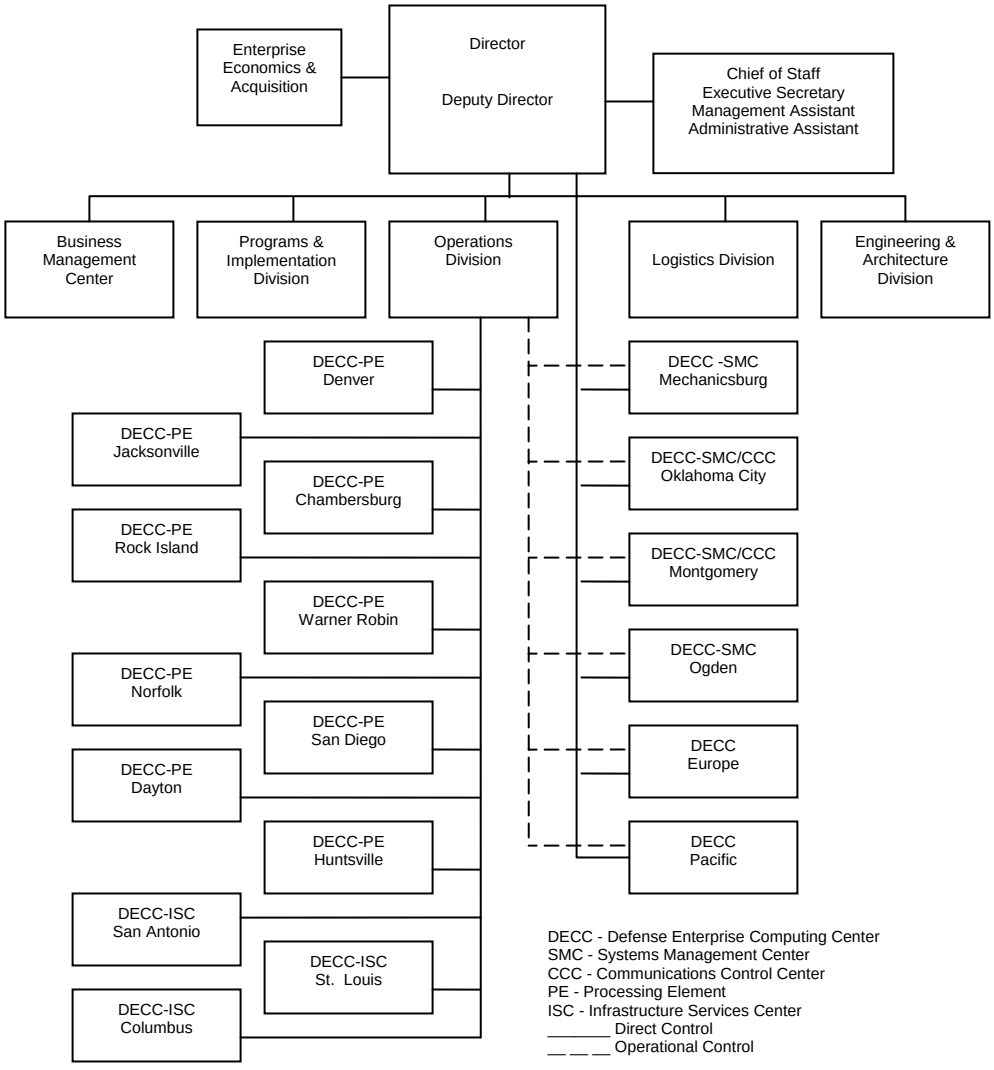
CS headquarters is located in Falls Church, Virginia. There are other headquarters elements located in Chambersburg, Pennsylvania; Denver, Colorado; Dayton, Ohio; and Pensacola, Florida. CS has a Director, Deputy Director, Chief of Staff, and two Special Advisors (one business and one technical), and the following five Divisions.

Business Management Center. The Business Management Center (BMC) provides budgeting, resource management, manpower, personnel, training, business proposals, and service-level agreements (SLA). There are three primary BMC elements: CS Headquarters in Falls Church, Virginia; the Blue Ridge Center located in Chambersburg, Pennsylvania; and the Rocky Mountain Center located in Denver, Colorado.

Programs and Implementation Division. The Programs and Implementation Division manages and directs assigned programs for CS. Programs include the migration of legacy systems to standard systems, development of standard business practices, and

definition of operational acquisition requirements. The Division Chief sets policy and procedures for CS project management and has subordinate branches for Implementation Support, Mainframe, Mid-Tier, and Communications. This division also has liaison personnel located at each of the Systems Management Centers (SMCs).

Chart 2. Center for Computing Services



Engineering and Architecture Division. The Engineering and Architecture Division conceives and develops alternative architectural strategies for adding new computer and telecommunications technologies into systems to increase system security, survivability, interoperability, endurance, and sustainability. This division directs and performs complex system engineering trade-off analyses for technology and facilities. The Engineering and Architecture Division has elements located in Falls Church, Virginia, and Denver, Colorado.

Logistics Division. The Logistics Division advises the Director of CS on all logistics, acquisition, and facilities management issues and provides command direction and guidance to execute integrated logistics support for assigned activities and systems. This

division manages logistics support for assigned operational elements of the Defense Information Infrastructure for the Directors of DISA and CS. The Logistics Division provides matrixed, cost-effective, integrated life cycle logistics and acquisition support services to CS. This division has offices in Chambersburg, Pennsylvania; Denver, Colorado; and Dayton, Ohio. The Logistics Division also has a liaison officer in each of the four SMCs.

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 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 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 the continental United States are divided into the following functional designations.

- **Systems 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, Pennsylvania; Montgomery, Alabama; Ogden, Utah; and Oklahoma City; Oklahoma.
- **Infrastructure Services Centers (ISCs)**. ISC personnel perform system management for specialized fielding efforts from CS customers. The ISCs are in Columbus, Ohio; St. Louis, Missouri; and San Antonio, Texas.

- **Processing Elements (PEs)**. Facility management, hardware support, physical security, touch labor[2] for communication devices, and touch labor for media management are the primary responsibilities for each PE. The PEs are located in Chambersburg, Pennsylvania; Dayton, Ohio; Denver, Colorado; Huntsville, Alabama; Jacksonville, Florida; Norfolk, Virginia; Rock Island, Illinois; San Diego, California; and Warner Robins, Georgia.

Communications Control Centers. The CCCs manage all classified and unclassified network devices. The CCCs are at DECCs Montgomery and Oklahoma City.

Field Security Operations

The mission of Field Security Operations (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 Computer Network Operations, 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 Designated Approving Authority (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.

Chief Information Officer

The Chief Information Officer (CIO) provides staff support in accomplishing information resources management duties mandated by the Clinger-Cohen Act. The CIO develops information resources management and information technology (IT) policies, performs IT management strategic planning, and incorporates and disseminates architecture and standards guidance, as well as IT investment criteria. The CIO advises on acquisitions for DISA IT and coordinates with Office of the Secretary of Defense on information resources management, IT, and IT acquisition matters. The CIO is the DAA for DISA-owned and -operated internal IT enclaves and networks. The CIO manages the agency-wide programs for Privacy Act and records management, and manages implementation of the DISA Electronic Business and Electronic Commerce.

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,

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

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.

Overview of the 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 customer expectations through professional and consistent operations services and standard implementation of DoD regulations and policies. CS is responsible for continual refinement and analysis of operations performance metrics and practices to identify and implement opportunities for improvement in executing core operations services and maintaining the integrity of the security posture of the operations environment.

Security Management

Security Review Program Guidance. In general, security review programs focus on management actions that establish the DAA and the processes that support the accreditation of an automated information system. DoD implemented the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," requirements for a security program through DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," dated December 30, 1997, and other DoD policies. DISA Instruction 630-230-19, "Automated Data Processing Information Systems Security Program," dated July 9, 1996, prescribes policy and assigns responsibilities for implementing, managing, and maintaining the DISA Information Systems Security Program and implements the DoD

programs, including DITSCAP and designation of the DAA. The DITSCAP and resultant Certification and Accreditation program are major components of the DISA security review program.

Security Control Program at the DECCs. The DISA Computing Services Security Handbook (the Security Handbook), the Information Assurance Vulnerability Alert Handbook, and the STIGs cover the Federal (OMB, DoD, and DISA) requirement for the primary operational-level guidance for implementation of automated information system security controls. The DECC security management organization structure and general business practices support the security program, including review of security controls.

Security Roles and Responsibility

DISA DAA/CIO. The DISA DAA/CIO retains the overall responsibility for the Certification and Accreditation as it pertains to the DITSCAP process of the CS sites.

CS Information Assurance Manager (IAM). The CS IAM provides guidance and advice to CS on IA, communications, and emanation security. This position is located within the FSO. However, the CS IAM reports to the Chief of Operations on security matters. When there is a disagreement relating to security, the CS IAM can go directly to the Deputy Director or Director of CS.

CS Security Manager (SM). The CS SM provides guidance and advice to the Director of CS, his staff, and personnel on physical, industrial, personnel, and information security, as well as security management. This position is located within the FSO, but reports to the Chief of Operations on security matters. When there is a disagreement relating to security, the CS SM can go directly to the Deputy Director or Director of CS.

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. The site IAM reports to the Deputy Director or Director of the site.

Site Information Assurance Officer (IAO). The site IAO assists the site IAM in meeting the duties and responsibilities discussed previously. The site IAO reports to the site IAM.

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. 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. The SRR and vulnerability scans 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 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 System Security Authorization Agreement under the DITSCAP by the DISA DAA (the DISA CIO). A complete formal review and documented risk assessment is conducted only every 3 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**. These systems handle 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.** These systems handle 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**. These systems handle information that is necessary for the conduct of day-to-day business, but do 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

The FSO and CS use automated scripts and the IA connection approval process to validate DISA compliance. The results are maintained in the Vulnerability Management System (VMS) and Security Automated Database databases. CS categorizes the findings or vulnerabilities into four categories, based on severity.

- **Finding Category I.** Any vulnerability that may result in a total loss of information or that provides 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 could lead to an unauthorized access.

- **Finding Category IV.** Any other vulnerability 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 3-year cycle to coincide with the formal accreditation cycle. The number of FSO visits is dependent on reviewing 33 percent of each site's assets on an annual basis. In accordance with DITSCAP, accreditation decisions are made for a maximum of a 3-year period. Annual reviews conducted by the FSO are known as Information Assurance Reviews. The Information Assurance Review includes a review of procedures, documentation, SRRs, and a vulnerability or penetration scan. All Information Assurance Review results are entered into VMS and briefed to the responsible senior management and security staff as well as the Director, CS.

System Readiness Reviews. The SRRs are manual (the traditional SRR) or automated checks (the technical SRR) and vulnerability scans.

Traditional SRR. The traditional SRR 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 SRR. The technical SRR uses automated checks of network devices, firewalls, intrusion detection systems, operating systems, databases, and web applications to verify that standard configuration settings are in accordance with applicable Security Technical Implementation Guides (STIGs).

Vulnerability Scans. The Vulnerability Assessment Process uses a commercial automated scanning tool, Retina Scan, that checks for known or demonstrated vulnerabilities. The scan is a 2-step process. The first step is external to the perimeter of the enclave and determines the robustness of perimeter defenses. The second step is inside the perimeter of the enclave and determines the robustness of the defense of each device within the enclave. Scan results; when associated with the communications, server, database, and web applications running on a device; have been adapted to feed into the SRR database, which is a part of the VMS database. When findings from the scan cannot be associated with a specific device, it is called a Vulnerability Assessment Process Report and is associated with the network of that enclave.

Internal Compliance Validation. There are two internal compliance validation processes. The first validation process is an automated review process that uses scripts developed by the FSO to test server compliance. Server operating systems managed locally and remotely by SMCs Mechanicsburg, Montgomery, Ogden, and Oklahoma City are subject to self-assessment automated scripts that are run on a weekly basis. The results are posted to the Security Automated Database, and remediation actions are tracked. The results of the reviews are forwarded to the appropriate SAs and their supervisors.

The second validation process is the IA connection approval process. The IA connection approval process uses FSO SRR scripts and checklists for servers, databases, and web services to complete self-assessments of new servers or software upgrades. The self-assessment results are fed into the SRR database and are forwarded to the connection approval authority for review and approval. To obtain approval, servers, databases, or web services must have no open Category I findings on the FSO SRR scripts and checklists, and at least 85 to 95 percent compliance[3] with all possible Category II and III findings. The senior person at the DECC SMC and DECC ISC is the approving authority for those organizations. The CS, Chief of Operations, is the approving authority for all DECC PEs and all CS Headquarters Divisions.

Vulnerability Databases. CS uses two databases to track vulnerabilities, VMS and Security Automated Database. VMS is maintained by the FSO, while the Security Automated Database is maintained by System Support Office (SSO) Montgomery. The two databases do not share information.

Vulnerability Management System. VMS is a DoD and DISA vulnerability management system. The DoD portion of the system is a database known as the Information Assurance Vulnerability Management database. The Information Assurance Vulnerability Management database is used by DoD to track acknowledgement and compliance with alerts released under the Information Assurance Vulnerability Management program as directed by Chairman of Joint Chiefs of Staff Instruction 6510-01D, "Information Assurance (IA) and Computer Network Defense." The DISA portion of VMS has two databases: one is the SRR database and the other is the Vulnerability Compliance Tracking System database.

SRR Database. The SRR database identifies SRR findings, tracks remediation of those findings, and has an automated waiver process for findings that cannot be fixed within an established timeframe. The CS IAM is responsible for checking VMS to determine who reviews open SRR findings and determines what the plan of action is to remediate the findings. The CS IAM also reviews requests for waivers to open SRR findings and renders a decision to the DISA approving authority.

Vulnerability Compliance Tracking System Database. The Vulnerability Compliance Tracking System database tracks DISA acknowledgement and compliance with the DoD Information Assurance Vulnerability Management[4] program. The Vulnerability Compliance Tracking System has a registry of all assets with associated operating systems and utility software, and identifies the owner of the asset and the responsible primary and alternate SAs. As alerts are released in the Information Assurance Vulnerability Management program, the Vulnerability Compliance Tracking System notifies the SA and IAM of alerts by e-mail. The SA is responsible for acknowledging receipt of the notification and updating the status of Information Assurance Vulnerability Management releases in the Vulnerability Compliance Tracking System.

The CS IAM is responsible for checking VMS to determine who is not in compliance with Information Assurance Vulnerability Management releases. The CS IAM notifies the responsible site IAM or IAO of any concerns or assets that are not in compliance within 7 working days of the compliance date. The Director of CS and primary staff are briefed on the status of compliance on a weekly basis. The CS IAM also reviews

[3] The percentage varies based on the technology.

[4] Includes alerts, bulletins, and advisories.

requests for extensions to compliance dates and recommends a concurrence or nonconcurrence to the approving authority, the DISA DAA. The FSO provides technical reviews for the CS IAM on request.

Security Automated Database. The Security Automated Database was created to track and remediate automated SRR self-assessment issues. The automated SRR program uses automated scripts developed by the FSO to conduct SRRs across the network using Secure File Transfer Protocol. The FSO has SRR scripts for all Windows, UNIX, LINUX, Oracle Database, and Standard Query Language databases and is moving toward running weekly SRRs on all servers, Oracle Databases, and Sequel Server Databases by the end of 2006. Automated SRR scripts are limited in that they cannot perform the manual checks of the STIGs. Automated SRR scripts test only the configuration settings of the hardware and software associated with the IT. Operating system scripts are capable of checking most of the configuration settings while the database scripts are capable of checking only approximately 35 percent of the configuration settings. The FSO and CS are working collectively on improving the SRR scripts and developing scripts for the other operating systems, the mainframe (IBM and Unisys) operating systems, and web software.

The security staff at the SMCs reviews and updates findings from the weekly automated SRR and monitors the remediation, especially any Category I and II findings. All Category I findings are entered in the trouble ticket system, Trouble Ticketing Management System, and flagged for immediate remediation. Site directors are briefed on the results of the automated scripts on a weekly basis and the Director, CS and primary CS staff are briefed on the results of the automated scripts on a monthly basis.

Information Assurance Monitoring

IA monitoring occurs at the enclave perimeters as well as within systems, database, and web software running within those systems. In addition to the external FSO reviews and the internal CS reviews, CS networks are also subject to monitoring by the Global Network Security Center as part of the GIG monitoring and internal network monitoring.

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 (the Center), are known as the Joint Intrusion Detection System. The Center monitors all Joint Intrusion Detection Systems on the GIG within the continental United States. Other centers are located around the world and all centers feed into a DoD Global Network Center Network Defense. This concept enables the Center to identify any information threat on an isolated, regional, or global basis. The Center notifies any element, to include CS, of any type of potential unauthorized attack or access. The Center also works with the CS CCCs and individual site 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 an access control list on the perimeter router, firewalls, and network IDS. The security staff located in the CCCs develops the security profiles for the enclave perimeter router, firewall, and network IDSs and monitors their respective reports and audit logs for unauthorized access or activities for the entire continental United States-based CS network. The security staffs 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 Computing Services Cell within the DISA

Network Operation Center and to the Center. The Center then directs all actions for this incident and closes it or turns it over to the appropriate investigative agency for action. The Computing Service Cell reports the incident to Computing Services Issue Center within the CS Operations Division.

The objective of layered defense is to provide a deny-by-default to the perimeter of the enclave. Deny-by-default can be defined as allowing those addresses, ports, protocols, accesses and actions that are authorized, while establishing a denial of those that are not authorized.

Enclave Monitoring. Security staff at the DECCs review system and database audit records at least weekly for suspicious actions. They perform preliminary inquiries with the customer, data owners, and others to determine the validity of suspicious actions. If an action cannot be validated, an unauthorized privilege is identified, or user-level action is identified, the action is reported to the Center and the CS Global Network Security Liaison Officer within the CS Operations Division.

Some of these sites also monitor the system and database audit reports using a host-based IDS. Validated unauthorized privilege or user accesses are reported up the same chain as the other incidents. All security incidents reported to the Computing Service Issue Center are briefed to the Director and Chief of Operations for CS every morning, Monday through Friday.

FSO Monitoring. The FSO conducts external vulnerability scanning twice a year for the NIPRNET and SIPRNET connections at all sites from Chambersburg. 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

Mainframes. In the mainframe environment, the IAO applies system security through the access control program. For the Unisys mainframe, the access control program is a product known as SIMON. The IBM mainframe Access Control Program products are Resource Access Control Facility, Access Control Facility 2, and Top Secret. The IAO also monitors security audit records to identify security concerns.

Servers. The SAs implement security for server, operating systems, databases, and web servers and web-based applications; primarily UNIX, Windows, Solaris, and Tandem. The IAO identifies each user's security profile, provides the SA with requirements, and then validates that the profile has been implemented as prescribed. The IAO also monitors security audit records to identify possible security concerns.

Personnel Controls

All civilian personnel are subject to Federal Civilian Personnel Systems. 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 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 the SAs. The SAs are required to have Secret clearance with IT-1 level.

All personnel security is managed and monitored by the CS SM in Chambersburg, in concert with site SMs. The CS SM submits all personnel security actions through the DISA Security Division. The DISA Security Division 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, fire detection, fire suppression, and climate control in accordance with national standards.

Electrical Distribution. Each site has 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.

Uninterrupted Power Supply. Each site has an uninterrupted power supply consisting of constantly charged batteries in case of power disruption. The uninterrupted power supply 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 problems. 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 at the entrances. In some case, 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 GSA-approved security containers.

Combinations to approved storage areas and security containers are restricted to only those who need to gain access, and a DISA Form 190A 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 Standard Form 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 opened and closed. Security containers are to be inspected daily and annotated on the Standard Form 702 to prevent security breach.

All classified transmissions that egress the perimeter router are encrypted using National Security Agency 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.

The Federal Information Processing Standards Publication 140-2, "Security Requirements for Cryptographic Modules," 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. National Security Agency devices are used for classified information and Federal Information Processing Standards Publication 140-2-compliant devices are used for unclassified information. All classified and unclassified information must be destroyed using approved methods of destruction in accordance with DoD Regulation 5200.1-R, "Information Security Program."

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 documentation 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.

Information and Communication

Information Systems Overview

The concept of operations for the CS emphasizes and describes a "customer focused" environment, organized with SMCs, Operations Support Teams, and production operations environments designed to provide a problem resolution and a situational awareness posture over all domains of a dynamic production environment that is operational 24 hours a day, 7 days a week, and 365 days a year.

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 applications, government off-the-shelf applications, customized legacy systems, web-based systems, voice-based systems including commercial telephone switch support, private branch exchange support, and multiple communications infrastructures. 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, CS Plan of the Week that summarizes various significant events, and the use of e-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, and every position description includes details of what responsibilities are required of the individual.

The CS BMC is responsible for Headquarters-level customer relations and acts as the point of contact for 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 CS Operations Division Network Operations 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.

Control Objectives and Related Control Activities

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

User Control Considerations

Computing Services User Controls

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

Customer User Controls

Customers are expected to have the following general user controls, at a minimum, built into their applications:

- individual user identification and
- individual user password or Public Key Infrastructure authentication.

The specific user controls are outlined in the individual customer SLAs.

Service-Level Agreements

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 relating to system access, security controls, data disposition and sharing, data encryption, and data backup for both CS and the customers.

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	DISA periodically assesses the appropriateness of security policies and procedures.	The FSO conducts annual Technical Interchange Meetings to assess the appropriateness of the STIGs.	Interviewed the FSO regarding the Technical Interchange Meeting process used to assess the appropriateness of the security policies such as the STIGs.	No relevant exceptions were noted.
1.2	Management monitors compliance with policies and procedures.	Monitor the currency of the security policies checked by the IAR process to accommodate new security policy requirements and technology changes.	Interviewed FSO personnel regarding their IAR process. Reviewed documentation prepared by FSO personnel indicating incorporation of security policy and technology changes into the IAR process.	No relevant exceptions were noted.
		SRRs are accomplished as a part of the IA review and certification and accreditation process. SRRs are performed by FSO and the site personnel.	Inspected 12 SRRs at the FSO to determine whether they were being performed. Interviewed SMC management to determine whether the SRRs were being performed.	No relevant exceptions were noted. At all four SMCs, SRRs performed by site personnel were permitted to be made exempt by the site SA, and the version of the SRR automated script program performed by that site did not match the SRR script program provided by FSO.
		FSO provides weekly reports on Information Assurance Vulnerabilities Alerts Category I and II to CS senior management.	Inspected a sample of ten Information Assurance Vulnerabilities Alerts reports issued by the FSO. Determined whether these reports were issued on a weekly basis.	No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
1.3	Corrective actions are effectively implemented.	Corrective actions to findings noted during the IAR are monitored through VMS by the IAM at the CS site and CS headquarters and by the certifying authority.	Interviewed the SMC IAMs and the FSO personnel or staff regarding their monitoring of vulnerabilities as recorded in the VMS system.	No relevant exceptions were noted.

Risk Assessments

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.	Enterprise risk assessments are prepared by CS based on the site risk assessment results.	Interviewed FSO personnel and the CS IAM to identify their procedures for preparing the enterprise-wide and site risk assessments and to determine whether risk assessments were documented.	No relevant exceptions were noted.
		Risk assessments are performed annually in accordance with DoD Instruction 5200.40.	Inspected the annual risk assessments for compliance with DoD Instruction 5200.40.	No relevant exceptions were noted.
		In accordance with the DoD and DISA guidance for Federal Information Security Management Act reporting, Plans of Action and Milestones (POA&Ms) are prepared by CS sites for all noncompliant, high-risk vulnerabilities, and are updated quarterly.	Inspected a sample of four Federal Information Security Management Act POA&M reports from the SMCs to determine whether all high-risk vulnerabilities listed in VMS were included.	Two SMCs did not submit POA&Ms for all noncompliance with high-risk vulnerabilities. Findings pertaining to self-assessments conducted by two SMCs were not uploaded as POA&Ms into the VMS.

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 current.**			
3.1	Site security plans are documented.	The security plan is documented by each CS site, addresses topics prescribed in OMB Circular A-130 and is on file at the DAA.	Obtained and inspected security plan documentation from the DAA for 17 DECCs for compliance with OMB Circular A-130 and DoD Instruction 5200.40.	Of 17 DECCs tested, 1 DECC did not have a security plan.
3.2	Site security plans are approved.	The security plan for all sites is signed by the senior official at the CS site.	Inspected the security plans or the site accreditation memos of 17 DECCs to determine whether they had been approved.	Of 17 DECCs tested, 1 DECC did not have a security plan.
3.3	Site security plans are current.	As part of the System Security Authorization Agreement (SSAA), the security plan is reviewed annually by the CS operations chief and updated as required.	Inspected the security plans for 17 DECCs to determine whether they had been reviewed annually by the CS operations chief and updated as required.	Of 17 DECCs tested, 1 DECC did not have a security plan. Security plans for two DECCs had not been reviewed and updated by the CS operations chief.

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.**			
4.1	A security management structure has been established with CS.	The "DISA Computing Services Enterprise Security – Roles and Responsibilities Concept of Operations," version 1.1, dated March 20, 2006,	Inspected the DISA Computing Services Enterprise Security Roles and Responsibilities Concept of Operations, March 20, 2006, version 1.1, to	No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
		defines the responsibilities of security officials at all levels in CS, to include FSO.	determine whether the responsibilities of security officials for all levels at CS and FSO have been defined.	
4.2	Information security responsibilities are clearly assigned.	The roles and responsibilities are outlined in the "DISA Computing Services Enterprise Security – Roles and Responsibilities Concept of Operations," version 1.1, dated March 20, 2006. The IAM, IAO, and SM are assigned through appointment orders.	Inspected appointment orders for 100 IAM, IAO, and SM positions at the SMCs and ISCs to assess the appropriateness and definition of roles. Compared appointment orders to the DISA Computing Services Enterprise Security Roles and Responsibilities Concept of Operations, March 20, 2006, version 1.1, for appropriateness and completeness.	Of 100 appointment orders tested, appointment orders for 16 IAM, IAO, and SM positions were neither complete nor compliant with the requirements defined in the DISA Computing Services Enterprise Security Roles and Responsibilities Concept of Operations, March 20, 2006, version 1.1. The exceptions were from two SMCs.
4.3	DISA employees are aware of security policies.	CS personnel are required to take initial security awareness training before gaining access to any system and required to take annual refresher security awareness training. MPS manages the training and records the completion for all CS Headquarters personnel located within the National Capitol Region. The training completion is recorded and maintained by the CS IAM or SM for all other CS personnel.	Inspected training records for a sample of 167 CS personnel at the SMCs, ISCs, and one headquarters element to determine whether the required training was completed timely and whether training records were maintained.	For 25 of 167 personnel tested, IA training was not completed prior to users being granted access to the system or training records were not maintained. The exceptions were from one SMC and one ISC.

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,	Personnel security checks are performed to determine that a valid and current personnel security investigation has been	Inspected a sample of 102 security background investigations for personnel at the SMCs and ISCs to determine	No relevant exceptions were noted

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
	hiring, transferring, and termination policies address security and are in compliance with DoD Instruction 8500.2.	conducted for each person at the site based on the individual's duties and tasks.	whether the investigations were valid and current.	
		The Security Handbook prescribes guidelines addressing position sensitivity designations for military and civilian employees.	Inspected the Security Handbook to determine whether position sensitivity designations for military and civilian employees were included.	No relevant exceptions were noted.
		Termination requires debriefing and revoking of all access. Termination debriefing (DISA Form 553) must be signed and maintained by the site security manager.	Inspected a sample of 36 terminated employees and contractors for the SMCs and one ISC to determine whether the employee's system access was revoked and whether a signed debriefing (DISA Form 553) was on file.	No relevant exceptions were noted.
		Security requirements for contractors are included in the contract requirements.	Inspected a sample of 45 contracts issued by the Defense Information Technology Contracting Organization to determine whether security requirements were included.	No relevant exceptions were noted.
		Personnel security compliance is monitored by CS security managers.	Interviewed the CS security manager at three SMCs to determine whether personnel security compliance was monitored.	No relevant exceptions were noted.
5.2	Job descriptions for government employees have been documented, and employees understand their duties and responsibilities.	All civilian positions have position descriptions.	Inspected a sample of 22 personnel files at 4 SMCs and 2 ISCs for civilian positions to determine whether the position descriptions existed.	No relevant exceptions were noted.
		All contractor job requirements are documented within the applicable contract.	Inspected a sample of 45 contracts issued by the Defense Information Technology Contracting Organization to	No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
			determine whether the documented contractor job requirements were included in the contracts.	
		Supervisors at all levels develop and maintain a performance plan for each individual and ensure that the plan requires that the employee's performance be based on the position description.	Inspected a sample of 36 employee performance plans at the SMCs and the ISC to determine whether the plans reflect the relevant position description.	Of 36 employee performance plans reviewed, 4 did not reflect the relevant position description. The exceptions were from one SMC and one ISC.
		Supervisors have access to staff position descriptions, and ensure that they correctly identify the task and functions of the position.	Interviewed supervisors of 25 sampled employees at 3 SMCs and 2 ISCs as to their awareness of the tasks and functions required of the employees. Compared their answers to the relevant position description for appropriateness.	No relevant exceptions were noted.
		CS management ensures that job descriptions and duties comply with DISA Instruction 220-15-55.	Interviewed MPS and CS management to determine whether they were in compliance with DISA Instruction 220-15-55.	No relevant exceptions were noted.
		Local written instructions may be followed for the performance of work.	Inspected a sample of 4 local written standard operating procedures at three SMCs for reasonableness in providing guidance for the performance of work.	No relevant exceptions were noted.
5.3	Employees (government and contractor) are adequately trained and possess the required skills.	SA certification requirements are established by DoD and DISA policies.	Interviewed FSO management regarding DoD and DISA policies used to establish SA certification requirements.	No relevant exceptions were noted.
		SA certification requirements are tracked by the FSO.	Inspected SA certification documentation tracked by the FSO for a sample of 112 SMC and ISC SAs to determine appropriateness and completeness of FSO data.	Certification documentation for 25 of 112 SAs tracked by the FSO was not complete. The 25 exceptions were from 2 SMCs.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
			Interviewed FSO personnel and the IAMs at the SMCs to determine whether SA privileges are reviewed annually.	No relevant exceptions were noted.
		Training requirements for IAMs and users are established by DoD and DISA policies.	Interviewed FSO and CS management regarding DoD and DISA policies used to establish training requirements. Inspected relevant DoD and DISA policies for appropriateness regarding training requirements.	No relevant exceptions were noted. No relevant exceptions were noted.
		Completion of the IAM and users training is tracked by the FSO and reviewed annually.	Interviewed FSO staff to determine the process for tracking SA certification requirements.	No relevant exceptions were noted.
5.4	Confidentiality or nondisclosure agreements are documented for all CS employees.	A nondisclosure statement is a required performance element for all employees.	Inspected a sample of 51 nondisclosure statements for personnel at the SMCs, ISCs, and one headquarters element to determine whether they were signed by the employee.	No relevant exceptions were noted.
5.5	Incompatible duties have been identified and policies implemented to segregate these duties.	The Security Handbook describes the segregation of duties of CS personnel. DISA CS Operations Policy Letter 06-15 "Segregation of Duties" describes the segregation of duties of CS personnel not outlined in the Security Handbook.	Inspected the CSD Operations Policy Letter CSD 06-15 "Segregation of Duties" and Security Handbook regarding the segregation of incompatible duties.	No relevant exceptions were noted.
		SLAs also describe the roles and responsibilities of CS in maintaining customer platforms.	Inspected a sample of 45 SLAs at the BMC to determine whether they describe the roles and responsibilities of CS for the maintenance of customer platforms.	No relevant exceptions were 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 criticality and sensitivity.** **Design Weakness:** CS did not have control procedures in place to ensure that information resources criticality and sensitivity were known and properly documented. Specifically, control procedures are needed to ensure the following: (a) customers define the criticality and sensitivity within the SLAs, (b) customers define the data disposition and data sharing process, and (c) customers sign the SLAs.			
6.1	Resource classifications and related criteria have been established.	Data owners are responsible for defining their information resources criticality in accordance with DoD Instruction 8500.2, and CS is responsible for documenting the criticality of the systems in the site SSAA, SLA, or VMS.	Inspected DITSCAP documentation for 17 DECCs to determine whether criticality of information resources established by data owners in accordance with DoD Instruction 8500.2 was documented by CS in the site's SSAA, SLA, or VMS.	Of 17 site DITSCAP packages tested, 3 did not define the criticality of information resources.
6.2	DISA has classified all DISA-owned assets according to criticality and sensitivity.	In accordance with DoD Directive 8500.1 and DoD Instruction 8500.2 system owners or customers establish the MAC level based on their assessment of the critical nature of their application or system.	Inspected a sample of 45 SLAs at the BMC to determine whether the documentation was completed in accordance with DoD Directive 8500.1 and DoD Instruction 8500.2 and system owners or customers included the MAC level.	Refer to item (a) of the design weakness. None of the 45 SLAs tested had MAC levels documented for their applications or systems.
		The site IAM has reviewed and accepted the criticality of the DISA-owned resources as defined by individual Authority to Operate or Interim Authority to Operate.	Inspected the SSAA information criticality for the SMCs for a DISA-owned resource to determine whether the site IAM has reviewed and accepted the criticality of the DISA-owned resource.	Two of the SMCs tested did not evidence the site IAM's review and acceptance of the criticality of DISA-owned resources.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
6.3	Customers classify their applications in the business proposal or SLAs.	CS customers communicate MAC levels to CS for their applications during the initial business proposal or in the SLA.	Requested initial business proposals and interviewed DISA personnel to determine whether MAC levels were included in initial business proposals. Inspected a sample of 45 SLAs at the BMC to determine whether the MAC level was communicated to CS by the CS customer.	MAC levels were not documented in initial business proposals according to DISA personnel. Refer to item (a) of the design weakness. None of the 45 SLAs and corresponding business proposals tested had MAC levels documented for their applications or systems.
6.4	Data management and the disposition and sharing of data requirements are identified in the SLAs.	The support agreement portion of the SLAs defines the data disposition and data sharing process.	Interviewed CS personnel at the BMC about the SLA process. Inspected a sample of 45 SLAs at the BMC to determine whether the support agreement portion of the SLA defines the data disposition and data sharing process.	Refer to item (b) of the design weakness. None of the 45 SLAs tested had a defined data disposition and data sharing process.
		SLAs are current and available in the Knowledge Management System.	Interviewed CS personnel at the BMC about the SLA update and approval process. Inspected a sample of 45 SLAs at the BMC to identify the date in which the SLA was updated and approved in accordance with CS policy. Observed the Knowledge Management System to determine whether the SLA was available.	Refer to item (c) of the design weakness. None of the 45 SLAs tested had evidence of approval signatures. No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
		If required by the customer, communications are secured by Type I or Type III cryptography devices.	Inspected a sample of 45 SLAs at the BMC to determine whether cryptography requirements existed and if so, observed the physical existence of the related Type I or Type III cryptography hardware and software.	No relevant exceptions were noted. None of the 45 SLAs tested had cryptography requirements.
		All requirements (if applicable) for communications secured by Type I or Type III cryptography devices are documented in the applicable SLA.	For the 45 SLAs sampled in the previous test, determined whether cryptography devices (both Type I and Type III) at each of the Oklahoma City and Montgomery CCCs existed.	No relevant exceptions were noted. None of the 45 SLAs tested had cryptography requirements.
6.5	CS has logical controls over data files and software programs.	If required by the customer where the data or the transmission of data needs to be protected, encryption tools such as Virtual Private Network, Secure Socket Layer, Secure Shell, and Public Key Infrastructure are used in accordance with DoD STIGs.	Inspected a sample of 45 SLAs at the BMC to determine whether the SLA requires encryption tools. For those SLAs that required encryption tools, observed the related hardware and software devices to determine whether the devices existed.	No relevant exceptions were noted. None of the 45 SLAs tested had encryption requirements.
6.6	CS correctly uses cryptographic tools.	All requirements (if applicable) for encryption are documented in the applicable SLA.	Inspected a sample of 45 SLAs at the BMC to determine whether encryption requirements, if applicable, are documented in the applicable SLA.	No relevant exceptions were noted. None of the 45 SLAs tested had encryption requirements.
		If required by the customer, DoD encryption policy is applied in accordance with Federal Information Processing Standards Publication 140-2.	Inspected a sample of 45 SLAs at the BMC to determine whether the DoD encryption policy was applied in accordance with Federal Information Processing Standards Publication 140-2 when required by the customer.	No relevant exceptions were noted. None of the 45 SLAs tested had encryption requirements.

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	Authorized owners and their access right are identified for DISA-owned assets.	In accordance with DoD Instruction 8500.2 and appropriate DoD STIGs, the site IAM or IAO maintains a list of all approved privileged user accounts created by CS SAs for operating systems, networks, databases, and web administrators.	Inspected the DD Form 2875 for a sample of 107 privileged users at the SMCs and ISCs, to determine whether the privileged users were approved.	No relevant exceptions were noted.
		Each privileged user identification issued is evidenced by a DD Form 2875, System Access Authorization Request (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 requires approval from the user's supervisor and validation of user personnel security investigation based on access requested.	Inspected a sample of 107 privileged users for the SMCs and ISCs to determine whether a DD Form 2875 (or its predecessor, DISA Form 41) was maintained by the data owner, approved by the user's supervisor or data owner and validated by the site security manager.	No relevant exceptions were noted
		The DoD Instruction 8500.2, as supplemented by CS Policy, details the process for granting access to system resources.	Inspected DoD Instruction 8500.2 and the Security Handbook to determine whether a process for granting access to system resources existed.	No relevant exceptions were noted.
7.2	IAOs or SAs periodically review authorization listings to determine appropriateness.	Periodic revalidation of DISA-managed systems, in accordance with applicable DoD STIGs and CS Policy, is conducted annually by the local IAM or IAO to identify privileged accounts and privileged user accesses that are no	Interviewed the IAM or IAO at the SMCs and ISCs and identified how the annual privileged account review is performed.	No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
		longer needed. (Customer rental space excluded.)	Inspected supporting documentation for the annual privileged account reviews at the SMCs and ISCs to determine whether the annual reviews were performed.	No relevant exceptions were noted.
7.3	Emergency and temporary access is controlled.	Emergency and temporary access authorizations are: • 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.	Interviewed CS personnel to determine whether CS had established policies and procedures for the creation and maintenance of emergency and temporary access to CS-owned or -administered systems. Interviewed CS personnel at the SMCs to determine whether emergency changes were made. For the two SMCs that had emergency changes, a sample of seven emergency and temporary user access requests was inspected to determine whether the 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.	No relevant exceptions were noted. No relevant exceptions were noted.

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) physical controls have been implemented.	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; • routine patrol and random door checks performed by the local military, DoD, or GSA guards in accordance with local base support agreement, if required; and • controlled access to the administrative areas by guard, mechanical cipher, or automated access control system.	Observed the physical inner and outer perimeters of the CS facility for 17 DECCs visited to determine whether: • individuals attempting to access the CS facility are required to present valid DoD identification; • perimeter security is in place to control vehicle and pedestrian access; • access to administrative areas is controlled by a guard, mechanical cipher lock, or automated access control system; and • routine patrol and random door checks are performed by local military, DoD, or GSA guards in accordance with applicable base support agreement(s).	No relevant exceptions were noted.
8.2	Building, administration, and computer facility physical controls have been implemented.	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 (for example, proximity card or DoD identification card) and something they know (for example, personal identification number) or something they are (for example, biometrics).	Observed access to the computer facility for 17 DECCs visited to determine whether such access requires positive identification of the employee through the use of something they have, for example, a proximity card or DoD identification card; something they know, for example, a personal identification number; or something they are, for example, biometrics.	Of 17 DECCs tested, 4 did not use 2-factor authentication to access the computer facility.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
		Employees must wear their picture identification cards above the waist.	Observed CS employees at 17 DECCs visited to determine whether picture identification cards are worn above the waist.	No relevant exceptions were noted.
		The area of the computer facility that contains unclassified equipment or information is in compliance with the requirements outlined in DoD Regulation 5200.8, for level C Restricted Areas, by having: • an electronic security system, • entry and circulation control, • barriers, and • security patrols or a designated response force.	Observed computer facilities containing the servers and related infrastructure for 17 DECCs visited to determine whether the security around the computer facility was in compliance with DoD Regulation 5200.8, for level C Restricted Areas, by having: • an electronic security system, • entry and circulation control, • barriers, and • security patrols or a designated response force.	No relevant exceptions were noted.
8.3	Visitors are controlled.	All CS site SMs must maintain an authorized access list to the CS facility.	Inspected access authorization documentation for a sample of 566 employees at the SMCs, ISCs, 7 PEs, and DECC Pacific to determine whether computer facility access was appropriate.	Access authorization documentation was not complete for 34 of 566 employees tested. The 34 employees were from 2 of 15 DECCs tested.
		Visitors who do not have the appropriate security investigation or clearance will be escorted at all times while in the computing facility.	Interviewed the site SM for 17 DECCs visited about the process for escorting visitors and the local site-specific badge color codes. Observed visitors with badges that require escort to determine whether such visitors were escorted at all times.	No relevant exceptions were noted. No relevant exceptions were noted.
		Visitors to the computing facilities that are not on the authorized access list must be validated by the local security manager, signed in and out of the facility, and escorted as required.	Interviewed the local security officer and security guard for 17 DECCs visited about handling visitors not on the authorized access list.	No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
			Observed visitors to CS facilities to determine whether the visitors were validated by the local security officer, signed in and out of the facility, and escorted as required.	No relevant exceptions were noted.
8.4	Traditional security reviews are performed.	As part of the site certification and accreditation process, a periodic traditional security review is conducted by the certifying authority at least every 3 years or more frequently based on the classification levels processed by the site.	Interviewed FSO personnel about the system classification levels and how they affect the traditional security review process and schedule. Inspected the traditional security review schedule provided by the FSO to determine whether the reviews were being performed in accordance with the system classification levels. Inspected DITSCAP documentation and the traditional security review for 17 DECCs to determine the date of the last traditional security review.	No relevant exceptions were noted. No relevant exceptions were noted. No relevant exceptions were noted.

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.	Password configuration requirements at the system level will be in compliance with appropriate DoD STIG.	Inspected system-generated documentation for a sample of 48 UNIX, 54 Windows, 20 mainframe, and 19 network devices managed by the SMCs and ISCs to determine whether the password configuration settings are in compliance with the appropriate DoD STIG.	Refer to item (a) of the design weakness. For 7 of 54 Windows, 23 of 48 UNIX, 7 of 19 network devices, and 3 of 20 mainframe computer systems tested, password configurations were not set in accordance with the appropriate DoD STIG.
		Passwords are checked for compliance with DoD STIG standards as part of the DISA-approved scanning tool, password- cracking utilities, or SRRs. Servers are checked with the automated scripts on a periodic basis. Schedule for annual reviews will be established locally in order to accommodate customer production, system maintenance, and system update or upgrade requirements.	Interviewed the IAM or SA at the SMCs to obtain an understanding of the process for checking compliance with DoD STIGs and for scheduling the annual reviews to accommodate customer production, system maintenance, and system update or upgrade requirements. Inspected supporting documentation for performing local SRRs.	No relevant exceptions were noted. No relevant exceptions were noted.
		Vendor-supplied default logons and passwords are removed, changed, or disabled in accordance with appropriate DoD STIG.	Inspected system-generated documentation for a sample of 48 UNIX, 54 Windows, 20 mainframe, and 19 network devices managed by the SMCs and ISCs to determine whether the vendor-supplied default logons and passwords were removed, changed, or disabled in accordance with the appropriate DoD STIG.	No relevant exceptions were noted.
9.2	Equipment and media are sanitized prior to disposal or reuse.	Sanitation of equipment and media prior to disposal or reuse are performed in accordance with DoD Regulation 5200.1-R, the Security Handbook, and the Assistant Secretary of Defense (Command, Control, Communications,	Interviewed CS operations staff at the SMCs to determine whether there was a process for compliance with DoD Regulation 5200 1-R and Security Handbook Section 3.5.	No relevant exceptions were noted.

		and Intelligence) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," dated June 4, 2001.	Reviewed logs at the SMCs for evidence of proper sanitation procedures.	No relevant exceptions were noted.
9.3	All access paths have been identified and controls have been implemented to prevent or detect access.	The operating system and communications software are configured to prevent circumvention of security software controls and unauthorized access from all paths.	Inspected system-generated documentation for a sample of 48 UNIX, 54 Windows, 20 mainframe, and 19 network devices managed by the SMCs and ISCs and, where available, other authorization (waiver) documentation to determine whether the operating system and communications software are configured to prevent circumvention of security software controls and unauthorized access from all paths.	Refer to item (b) of the design weakness. For 67 of 141 computer systems tested, operating system and communications software were not configured in accordance with the appropriate STIGs to prevent circumvention of security.
		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.	Inspected the network diagram for the CCCs to determine whether the diagram 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.	No relevant exceptions were noted.
		System software is configured in accordance with the DoD STIGs.	Inspected system-generated documentation for a sample of 48 UNIX, 54 Windows, 20 mainframe, and 19 network devices managed by the SMCs and ISCs and, where available, other authorization (waiver) documentation to determine whether the systems software was configured in accordance with DoD STIGs and CS policies.	Refer to item (b) of the design weakness. For 67 of 141 computer systems tested, systems software was not configured in accordance with the appropriate DoD STIGs and CS policies.

		Access to data files, software programs, and databases is controlled by the configuration setting as described in accordance with the DoD STIGs.	Inspected system-generated documentation for a sample of 48 UNIX, 54 Windows, 20 mainframe, and 19 network devices managed by the SMCs and ISCs and, where available, other authorization (waiver) documentation to determine whether access to data files, software programs, and databases is controlled by the configuration setting as describe in accordance with the DoD STIGs.	Refer to item (b) of the design weakness. For 67 of 141 computer systems tested, systems software was not configured in accordance with the appropriate DoD STIGs.
		Network diagrams are developed and maintained by the CCC to show potential access paths.	Inspected the network diagram for the CCCs to determine whether the potential access paths are indicated.	No relevant exceptions were noted.

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 capabilities are implemented.	CCC sites will maintain a current drawing of their network topology that includes all external and internal links, subnets, and network equipment in accordance with DoD STIGs.	Inspected the network topology for the CCCs to determine whether all external and internal links, subnets, and network equipment in accordance with DoD STIGs are included.	No relevant exceptions were noted.
		Dial-in telephone numbers are not published and are periodically changed.	Interviewed the IAM or SM for the SMCs about the process to control dial-in telephone numbers from being published.	No relevant exceptions were noted.
		Telecommunications access is controlled by the managing CCC for the network devices, including firewall and network	Interviewed network management staff at the CCCs about their process to manage the network devices. Inspected	No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
		IDSs, for all sites within the continental United States for unclassified wide-area networks. CCC personnel have access to those networks through the out-of-band virtual private network tunnel for all networks so equipped.	the network topology at the CCCs to determine whether the management of these network devices is restricted to the out-of-band private network.	
10.2	Network defense capabilities are implemented.	Network access paths are configured to prevent circumvention of security and unauthorized access, in accordance with DoD STIGs.	Attempted to access the network internally and externally at the SMCs to determine whether access paths were configured to prevent circumvention of security and unauthorized access, in accordance with DoD STIGs.	Networks at the SMCs were not configured to prevent circumvention of security and unauthorized access, in accordance with DoD STIGs
		Networking equipment is configured in accordance with DoD STIGs	Inspected system-generated documentation for a sample of 19 network devices managed by the SMCs and ISCs and, where available, system-generated documentation and other authorization (waiver) documentation to determine whether the devices were controlled by the configuration setting as promulgated by DoD STIGs.	Of 19 network devices tested, 7 were not configured in accordance with DoD STIGs.
10.3	Remote and dial-up capabilities are controlled.	Remote access is established in accordance with DoD STIGs.	Inspected user access agreements for a sample of 180 users at the 3 SMCs with remote access privileges to determine whether: • the signed agreement includes the type of access required by the user; • the signed agreement includes the responsibilities, the liabilities, and security measures (for example, malicious code detection training) involved in the use of their remote	Of 180 users tested, 35 did not have the appropriate authorization for remote access. The 35 users were from 3 SMCs.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
			access device; • incident handling and reporting procedures are identified along with a designated point of contact; • the remote user can be held responsible for damage caused to a Government system or data through negligence or a willful act; • the policy contains general security requirements and practices and will be acknowledged and signed by the remote user; • Government-owned hardware and software will be used for official duties only; and • the user is the only individual authorized to use this equipment. Inspected the authentication mechanism for remote access for three SMCs to determine whether a 2-factor authentication method was in place.	The three SMCs tested did not use 2-factor authentication for remote access.

Incident Response

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
11	**Controls provide reasonable assurance that an effective incident response capability has been implemented.**			
11.1	Incident response controls are implemented at DISA.	The DISA Instruction 360-225-1 provides guidance on handling incidents, incident reporting structure, and prioritization of incidents that are consistent with attributes noted in DoD Instruction 8500.2. Trouble Management System tickets or e-mails	Inspected documentation for a sample of 242 incidents at the SMCs and 2 ISCs to determine whether the questionnaire was completed in accordance with DISA CS Instruction 360-225-1. Specifically, the following items from the Trouble Management System questionnaire were	Of 242 incidents at the SMCs and 2 ISCs tested, 51 incident reports were not completed in accordance with DISA CS Instruction 360-225-1.

		are used as incident response and reporting tools for CS. Specifically, the following items from the Trouble Management System questionnaire must be completed. • What was the root cause of the problem? • What troubleshooting efforts were conducted? • Were redundant systems available and working? • Confirm overall impact the outage has on the customer mission. • Were scheduled batch processing jobs delayed? • If the reporting site remotely manages the application or equipment that has the problem, provide physical location of the equipment and application.	inspected. • What was the root cause of the problem? • What troubleshooting efforts were conducted? • Were redundant systems available and working? • Was overall impact of the outage on the customer's mission confirmed? • Were scheduled batch processing jobs delayed? • If the reporting site remotely managed the application or equipment that has the problem, was the physical location of the equipment and application provided?	

Access Monitoring

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
12	**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.			
12.1	Audit trails are maintained.	System auditing is enabled in accordance with DoD STIGs.	Inspected system-generated documentation for a sample of 141 computer systems to determine whether	Of the 141 systems tested, system auditing was not enabled for 23 systems and system permission settings for

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
			system auditing is enabled in accordance with DoD STIGs.	auditing logs were not configured correctly for 10 systems.
		System auditing review is in accordance with DoD STIGs.	Interviewed the SAs at the SMCs and ISCs to determine whether system auditing is reviewed in accordance with DoD STIGs.	Refer to the design weakness. At two SMCs and two ISCs, there was no periodic, scheduled review of audit logs.
		Auditing is conducted in accordance with DoD STIGs.	Interviewed the SAs at the SMCs and ISCs to determine whether system auditing is conducted in accordance with DoD STIGs.	Refer to the design weakness. At two SMCs and two ISCs, there was no periodic, scheduled auditing conducted.
12.2	Actual or attempted unauthorized, unusual, or sensitive network access is monitored.	Network intrusion detection systems used to monitor unusual or inappropriate activity are installed in accordance with the DoD STIGs.	Interviewed CCC staff and inspected the CCC network diagram to determine whether an external network intrusion detection system is installed and implemented and whether all external connections are monitored. Interviewed CCC staff and inspected the CCC network diagram to determine whether an internal network intrusion detection system (IDS) is installed and implemented and whether all internal connections are monitored.	No relevant exceptions were noted. No relevant exceptions were noted.
		Procedures are in place for monitoring, investigating, and reporting inappropriate or unusual activity. The DoD STIG outlines what activity constitutes inappropriate or unusual activities.	Interviewed the IAM, IAO, or SM at the CCCs to gain an understanding of the process followed when monitoring, investigating, and reporting inappropriate or unusual system activity. Inspected the site's network monitoring policy at the CCCs to determine whether the policy was in accordance with DoD STIGs and whether the policy identified	No relevant exceptions were noted. No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
			thresholds for an inappropriate or unusual event.	
12.3	Suspicious network access activity is investigated and appropriate action is taken.	Suspicious access activity is investigated and appropriate action taken in accordance with DISA Instruction 360-225-1 and CS Policy Letter CSD 06-02.	Interviewed CCC staff to determine whether suspicious network activity is investigated and appropriate action taken.	No relevant exceptions were noted.

Change Control

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
13	**Controls provide reasonable assurance that changes to DISA-owned assets are properly controlled.**			
13.1	DISA-initiated software or hardware modifications are authorized, and the documentation is maintained.	For customer-requested changes: In accordance with CS Change and Configuration Concept of Operations, proposed changes to hardware, operating system, utility software, communications, and networks are reviewed and approved. Local Change Control Boards are in place at each of the SMCs and two ISCs to oversee the change review and approval process. The site IAM is a voting member of the local Change Control Boards.	Inspected documentation for a sample of 175 change requests at the SMCs and two ISCs to determine whether changes are reviewed and approved in accordance with the CS Change and Configuration Concept of Operations, local Change Control Boards are in place at the SMCs and ISCs, and the IAM is a voting member of the Change Control Board.	Of 175 change requests, 3 were not approved by a supervisor or the local Change Control Board. The exceptions were from 1 SMC and 1 ISC
		Verification and acceptance of operating systems and utility software changes is documented and approved, and operating systems and utility software movements are controlled. The Executive Software Change Control Board (the Board)	Interviewed change management staff at the SMCs to determine the various change management roles and responsibilities, including the Board and Software Factory.	No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
		provides this control for operating systems and utility software DISA wide. Local change management controls the implementation of operating systems and executive software changes at the SMC and ISC level. All Board actions are documented and approved. Minutes of each Board meeting are published, and all documentation is maintained indefinitely and is available online or upon request. The actual movement of IBM mainframe software is tightly controlled by the Board and Software Factory interface. All software distributed by the Software Factory is tracked, notifications are provided to appropriate organizations, and a complete audit trail is retained.	Inspected the Board operating procedure document outlining the role of the Board to determine whether the Board controls the utility and operating system changes for four sites. Inspected evidence to determine whether all Board actions are documented and approved, and whether the minutes of Board meetings are available. Inspected the System Software Office product procedure installation guide for the mainframe systems at one site to determine whether all software distributed by the Software Factory is tracked, notifications are provided to appropriate organizations, and a complete audit trail is retained.	No relevant exceptions were noted. No relevant exceptions were noted. No relevant exceptions were noted.
13.2	New and modified hardware and operating system or utility software is tested and controlled according to specific criteria.	New systems and changes to existing systems are reviewed by an approving authority prior to connection to the network in accordance with CS Policy Letter CSD 05-09.	Inspected documentation for a sample of 128 change requests for new and existing systems at the SMCs to determine whether changes are reviewed by an approving authority prior to connection to the network.	No relevant exceptions were noted.
		Changes to hardware and operating systems software are documented in the minutes of the Change Control Board.	Inspected a sample of 74 Change Control Board meeting minutes for three SMCs and one ISC where the control is applicable to determine whether hardware and operating systems software changes are documented.	No relevant exceptions were noted.
		As part of the SSOPAC process for IBM mainframe operating system software	Interviewed System Software Office management personnel for the IBM	No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
		releases: • integration testing is performed to ensure functionality; • performance and stress testing is performed, as required, to identify impacts on system performance; and • security testing is performed for each operating system software release. Based upon test results, actions are initiated to rectify identified software deficiencies, performance impacts, and security problems.	mainframes based at DECC Mechanicsburg to determine the process for performing integration tasking, performance and stress testing, and security testing on IBM mainframe operating system releases.	
13.3	Emergency changes are promptly approved.	Emergency change procedures are documented in the CS Change and Configuration Management Plan.	Inspected the CS Change and Configuration Management Plan to determine whether emergency change procedures are defined and documented. Inspected documentation for a sample of 96 emergency changes at 3 SMCs and 1 ISC to determine whether: • the emergency changes were recorded and approved by management; and • normal change request forms and related documentation were completed after the emergency change occurred. Inspected documentation for a sample of 78 emergency changes at 3 SMCs to determine whether an independent review of each change was performed.	No relevant exceptions were noted. Of 96 emergency changes tested, 2 changes at 1 SMC were not approved by management. For eight emergency changes at one SMC, no independent review was documented.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
13.4	Movement of programs and data among libraries is controlled.	Mainframe Executive Software products are recorded and tracked. Inventories are maintained, which include version, maintenance level, out-of-support date, and documentation.	Inspected system documentation from the Mechanicsburg Software Factory for mainframe systems to determine whether mainframe executive software programs are recorded and tracked, and an inventory is maintained that includes the version, maintenance level, out-of-support date, and related documentation.	No relevant exceptions were noted.
13.5	Use of public domain and personal software is restricted.	Use of personal and public domain software on Government equipment is in accordance with DoD Directive 8500.1 and CS Operations policy.	Inspected the contents of 56 employees' computers at the SMCs and ISCs to determine whether the computers contained public domain and personal software not approved in accordance with DoD Directive 8500.1 and CS Operations policy.	Of 56 sampled computers, 35 computers at the 4 SMCs and 2 ISCs contained unapproved, public domain or personal software.

Service Continuity

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
14	**Controls provide reasonable assurance that procedures and controls are in place to prevent or minimize unexpected interruptions.**			
14.1	Data and program backup procedures have been implemented.	Each site has implemented its own off-site and transportation agreements in accordance with SLA requirements.	Interviewed computer center operations staff at the SMCs and ISCs to determine their off-site and transportation requirements for backup media. Inspected the off-site transportation agreement for the SMCs and ISCs to determine whether backup media is transported to the off-site location in accordance with SLA requirements.	No relevant exceptions were noted. No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
		Data and program backup procedures are conducted in accordance with the appropriate DoD STIGs, SLA requirements, and CS Policy Letter 06-01.	Inspected the off-site transportation agreement for the SMCs and ISCs to determine whether the agreement included the following: • a schedule for the weekly full data backup; • a schedule for an incremental daily backup; • a schedule for monthly full system backup; • detailed backup procedures; • a plan for rotating backup media; • detailed restoration procedures; • customer requirements, a copy of a memorandum of agreement, and a copy of any SLA; • storage and retention procedures for backup media; • schedule and methodology for testing restoration procedures; • procedures for maintaining a historical file for the "root" password in a controlled access environment; and • backup procedures that are tested at least annually.	No relevant exceptions were noted.
			Interviewed staff and inspected documentation for the SMCs and ISCs to determine whether data and program backup procedures are in compliance with DoD STIGs, SLA requirements, and CS Policy Letter 06-01.	No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
14.2	Environmental controls have been implemented.	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 only 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.	Interviewed data center personnel and inspected the data center for the 17 DECCs to determine whether the following environmental controls were in place: • fire detection, prevention, and suppression mechanisms; • air conditioning, temperature, and humidity control systems; • uninterrupted power supplies, voltage regulators, and backup generators.	At one DECC, no agreement could be located to demonstrate firefighting support provided by the base. At two DECCs, a copy of the last fire marshal inspection was not available. At one DECC, the fire department is not automatically notified in case of fire.
		All 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 operating	Interviewed data center personnel and inspected the data center for the 17 DECCs 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, • automatic voltage control systems, • a minimum of two electrical feeds, • battery powered uninterrupted power system, and	One DECC did not have humidity control devices installed.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
		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; and backup generators that are set to automatically start 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.	• backup generators that are set to automatically start.	
14.3	Hardware maintenance controls have been implemented.	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.	Interviewed computer operations staff for the SMCs and ISCs to determine the process for scheduling preventive maintenance on facilities equipment and tracking completion of scheduled maintenance.	At one ISC, testing of the water sensors was not conducted to determine if the sensors are operable.
		Records are maintained on the actual performance in meeting facilities equipment service schedules.	Interviewed operations and facility management to determine the process for scheduling, monitoring, and tracking completion of maintenance on facilities equipment.	No relevant exceptions were noted.
		Policies and procedures for IT equipment maintenance exist and are up-to-date.	Inspected the IT equipment maintenance policies and procedures at CS Logistics to determine whether the policies and procedures exist and are up-to-date.	No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
		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.	Interviewed computer operations staff at the SMCs and ISCs to determine the process for scheduling, monitoring, and tracking completion of maintenance on IT equipment. Inspected 255 IT equipment maintenance tickets at the SMCs and 1 ISC to determine whether scheduled maintenance is completed.	No relevant exceptions were noted. No relevant exceptions were noted.
		Regular and unscheduled maintenance on IT equipment is performed and documented.	Interviewed computer operations staff for the SMCs and ISCs to determine the process for scheduling maintenance on IT equipment and documenting completion of scheduled maintenance.	No relevant exceptions were noted.
		Flexibility exists in the data processing operations to accommodate regular and a reasonable amount of unscheduled maintenance.	Interviewed computer operations staff for the SMCs and ISCs on their process for determining flexibility in the data processing operations to accommodate a regular and reasonable amount of unscheduled maintenance.	No relevant exceptions were noted.
		Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	Interviewed computer operations staff for the SMCs and ISCs to determine whether spare or backup hardware inventory existed.	No relevant exceptions were noted.
		Goals are established by senior management on the availability of data processing and on-line services.	Interviewed site management at CSD Headquarters and CDS Operations to determine whether availability goals are established and documented for data processing and on-line services.	No relevant exceptions were noted.

No.	Control Objectives	Control Techniques	Test of Operating Effectiveness	Results of Testing
		Records are maintained on the actual performance in meeting IT equipment service schedules.	Interviewed operations management to determine the process for scheduling, monitoring, and tracking completion of scheduled maintenance on IT equipment.	No relevant exceptions were noted.
		Regular and unscheduled maintenance on facilities equipment is performed and documented.	Interviewed computer operations staff for the SMCs and ISCs to determine the process for scheduling, monitoring, and tracking completion of maintenance on facilities equipment, preventive maintenance procedures and schedule.	No relevant exceptions were noted.
14.4	Staff have been trained to respond to emergencies.	Data center staff receive periodic training in emergency fire, flooding, and alarm incident procedures.	Inspected training documentation for 105 employees at 3 SMCs and the ISCs to determine whether the employees had received training in emergency fire, flooding, and alarm incident procedures.	Formal emergency response training has not been conducted on a regular basis. Of 105 employee records reviewed, 29 at 2 ISCs did not complete the training.
		Data center employees have received training and understand their emergency roles and responsibilities.	Inspected training documentation for 105 employees at 3 SMCs and the ISCs to determine whether they had received training in emergency roles and responsibilities.	Of 105 employees, 29 at 2 ISCs did not complete formal training on their emergency roles and responsibilities.
		Emergency procedures are periodically tested.	Inspected emergency plan and test documentation for the SMCs and ISCs to determine whether the test was performed annually and whether the results were documented.	No relevant exceptions were noted.
		Emergency response procedures are documented.	Inspected emergency response procedures for the SMCs and ISCs to determine whether they were documented.	No relevant exceptions were 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 awaiting implementation of the DoD-wide, host-based security solution.

2006 Results of Testing Requiring DoD or DISA Enterprise Solutions

Vulnerability Management System (VMS). The 2006 Statement on Auditing Standards No. 70 project included results of testing that indicated noncompliance with DoD STIGs and POA&Ms. It is significant to note that the tool used to track vulnerabilities (VMS 6.0), originally scheduled to be implemented in December 2005, was delayed until May 2006, in the middle of the diagnostic testing phase of the audit. Because all CS controls and control techniques were developed and implemented based on an operational VMS 6.0, several gaps were observed in POA&M documentation (a new requirement for VMS 6.0) that support actions and mitigations for identified vulnerabilities. In short, the majority of POA&M findings in this area are attributable to the VMS upgrade from 5.4 to 6.0 and do not indicate a lack of CS enforcement of the DoD STIGs and CS policy regarding POA&Ms.

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

Processing Elements
- Chambersburg, Pennsylvania
- Dayton, Ohio
- Denver, Colorado
- Huntsville, Alabama
- Jacksonville, Florida
- Norfolk, Virginia
- Rock Island, Illinois
- San Diego, California
- Warner Robins, Georgia

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.

Paul J. Granetto
Patricia A. Marsh
Patricia C. Remington
Suzette L. Luecke
Anh Tran
Michael L. Davitt
Chi H. Lam
Chanda D. Lee-Baynard
Danial Olberding
Ernest Fine
Minh Tran
Wen-Tswan Chen
Christopher Bitakis