

September 6, 2005



# Information Technology Management

Report on Defense Information Systems Agency,  
Center for Computing Services Controls Placed in  
Operation and Tests of Operating Effectiveness  
for the Period October 1, 2004 through April 30,  
2005 (D-2005-105)

Department of Defense  
Office of the Inspector General

Constitution of  
the United States

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

Article I, Section 9

### **Additional Copies**

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

### **Suggestions for Future Audits**

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

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

DEPARTMENT OF DEFENSE

**hotline**

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

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



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

September 6, 2005

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

SUBJECT: Report on Defense Information Systems Agency, Center for Computing  
Services Controls Placed in Operation and Tests of Operating Effectiveness  
for the Period October 1, 2004 through April 30, 2005  
(Report No. D-2005-105)

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

We appreciate the courtesies extended to the staff. Questions should be directed to Mr. Michael Perkins at (703) 325-3557 (DSN 221-3557) or 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  
Defense Financial Auditing  
Service

# Table of Contents

---

<b>Forward</b>	i
<b>Section I</b>	
Independent Service Auditors' Report	1
<b>Section II</b>	
Overview of Operations	9
Overview of Control Environment	14
Information and Communication	25
Control Objectives and Related Control Activities	26
User Control Considerations	26
<b>Section III</b>	
Entity-wide Security Program	31
Access Control	37
Software Development and Change Control	50
Segregation of Duties	55
Service Continuity	59
<b>Section IV</b>	
Introduction	65
Security Processes and Other Considerations	69
Continuity of Operations Plan	70
Summary	71
<b>Acronyms and Abbreviations</b>	72
<b>Report Distribution</b>	73

## **FOREWARD**

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 Officer's Act of 1990 (P.L. 101-576), as amended, mandates that agencies prepare and conduct audits of financial statements. The reliability of information processed at DISA sites directly impacts DoD's ability to produce reliable, and ultimately auditable, financial statements, which is key to achieving the goals of the Chief Financial Officer's Act.

This report focuses on DISA's Center for Computing Services (CS), an organization that 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-owned and customer-owned platforms to include computer operations, data storage, systems administration, security management, capacity management, system engineering, web and portal hosting, architectural development, and performance monitoring.

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

The concept of internal controls is fundamental to this Statement on Auditing Standards No. 70 report. Internal control is the process designed to provide reasonable assurance that objectives regarding the reliability of financial reporting, the effectiveness of operations, and compliance with applicable significant laws and regulations are achieved. DISA has imposed internal control standards that require strict compliance with DoD and DISA policies. DISA's level of compliance with specific aspects of these regulations has a direct impact on the accompanying description of internal controls and related test results.

---

## **Section I: Independent Service Auditors' Report**

---





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

September 6, 2005

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

SUBJECT: Report on Defense Information Systems Agency Controls Placed in  
Operation and Tests of Operating Effectiveness for the Period October 1,  
2004 through April 30, 2005

We have examined the accompanying description of Defense Information Systems Agency (DISA) Center for Computer Services (CS) controls applicable to the Defense Enterprise Computing Centers (DECCs) located at Chambersburg, Pennsylvania; Columbus, Ohio; Dayton, Ohio; Denver, Colorado; Huntsville, Alabama; Jacksonville, Florida; Mechanicsburg, Pennsylvania; Montgomery, Alabama; Norfolk, Virginia; Oklahoma City, Oklahoma; Ogden, Utah; Rock Island, Illinois; San Antonio, Texas; San Diego, California; St. Louis, Missouri; and Warner Robins, Georgia. These locations and the unclassified technologies (operating systems) resident therein were the sample population from which tests of specific controls were applied. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of CS's information technology (IT) controls that may be relevant to a user organization's internal controls as it relates to an audit of financial statements; (2) the IT 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 CS's controls; and (3) such controls had been placed in operation as of April 30, 2005. The control objectives were specified by the Office of Inspector General, Department of Defense. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and the standards applicable to financial audits contained in Government Auditing Standards issued by the Comptroller General of the United States, and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

As discussed in the accompanying description, CS did not have control procedures in place to ensure that resource owners identified authorized users and their respective access rights. These deficiencies resulted in controls not being suitably designed to achieve control objective AC 2, "Controls provide reasonable assurance that a current list of authorized users and their respective access rights are maintained."

As discussed in the accompanying description, CS did not completely have DoD required logical control procedures in place to fully ensure passwords, tokens, or other devices were used to identify and authenticate users; access paths were identified and access authorizations were appropriately limited; policies and techniques had been implemented for using and monitoring the use of system utilities, as well as for investigating and resolving inappropriate or unusual activity; telecommunications were secured; and cryptographic tools were used in a secure fashion. These deficiencies resulted in the implementation, monitoring, and enforcement of logical controls not being suitably



designed to achieve control objective AC 3, “Controls provide reasonable assurance that physical and logical controls to prevent or detect unauthorized access are fully established and access to and use of system software is monitored.”

As discussed in the accompanying description, control procedures in place by CS did not fully ensure audit trails were always maintained and actual or attempted unauthorized, unusual, or sensitive access was fully monitored. These deficiencies resulted in controls not being suitably designed to achieve control objective AC 4, “Controls provide reasonable assurance that access is monitored, apparent 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 CS controls that had been placed in operation as of April 30, 2005. Also, in our opinion, except for the matters described in the preceding paragraphs, the controls, as described, were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily.

CS states in its description of controls that all security risks are periodically assessed against federal requirements. Tests of operating effectiveness indicated that not all risk assessments fully conformed to the Field Security Operations (FSO) Risk Analysis Guide. As a result, the control objective SP 1, “Controls provide reasonable assurance that security risks are periodically assessed,” was not achieved.

CS states in its description of controls that all security plans are kept current. Tests of operating effectiveness indicated that not all security plans incorporated current guidance provided by DoD Instruction 8500.2, the DISA Computing Services Handbook, and Office of Management and Budget (OMB) Circular A-130 Appendix III. As a result, control objective SP 2, “Controls provide reasonable assurance that an entity-wide security program plan is documented, approved, and kept current,” was not achieved.

CS states in its description of controls that owners and users are aware of security policies and that an incident response capability has been fully implemented. Tests of operating effectiveness indicated that not all sites had an effective security awareness program that provided guidance to users regarding the importance of security, not all sites had procedures implemented to determine that employees and contractors completed a nondisclosure agreement form to evidence their understanding and acceptance of confidential information disclosure restrictions and requirements, and not all site personnel were familiar with their responsibilities for intrusion detection and incident response. As a result, control objective SP 3, “Controls provide reasonable assurance that a security management structure is established and security responsibilities are clearly assigned,” was not achieved.

CS states in its description of controls that hiring, transfer, termination, and performance policies address personnel security and that employees have adequate training and expertise. Tests of operating effectiveness indicated that not all sites implemented formal policies for debriefing and removing access of terminated employees, not all sites provided appropriate training for personnel to perform their duties, and not all sites maintained documentation of employee training and professional development activities. As a result, control objective SP 4, “Controls provide reasonable assurance that effective security-related personnel policies have been implemented,” was not achieved.

CS states in its description of controls that authorizations for software modifications are documented and maintained and the use of public domain and personal software is

restricted. Tests of operating effectiveness indicated that not all sites always documented configuration change request authorizations and not all sites restricted the use of unapproved and unaccredited software. As a result, control objective CC 1, "Controls provide reasonable assurance that processing features and program modifications are properly authorized," was not achieved.

CS states in its description of controls that changes are controlled as software progresses through testing to final implementation. Tests of operating effectiveness indicated that not all sites restricted programmers' access to the production environment, and not all sites maintained adequate audit trails or logs for identified systems. As a result, control objective CC 2, "Controls provide reasonable assurance that all new and revised software including system software are tested and controlled," was not achieved.

CS states in its description of controls that movement of programs and data among libraries is controlled. Tests of operating effectiveness indicated that not all sites had complete procedures for movement of program code between libraries, as well as complete documentation and approval processes. As a result, control objective CC 3, "Controls provide reasonable assurance that software libraries are controlled," was not achieved.

CS states in its description of controls that data and program backup procedures and environmental controls have been implemented. Tests of operating effectiveness indicated that not all sites had formal tape backup procedures that were being consistently followed; performed backup verifications; procedures to recover backups stored off-site; procedures to control physical access to off-site locations; sufficient environmental controls; and trained environmental personnel. As a result, control objective SC 2, "Controls provide reasonable assurance that data and program backup procedures and environmental controls have been implemented," was not achieved.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in section III, to obtain evidence about their effectiveness in meeting control objectives, described in section III, during the period from October 1, 2004 to April 30, 2005. The specific controls and the nature, timing, extent, and results of the tests are listed in section III. 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 of user organizations, when making assessments of control risk for user organizations.

In our opinion, except for the deficiencies listed in the preceding paragraphs, the controls that were tested, as described in section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in section III were achieved during the period from October 1, 2004 to April 30, 2005; however, the scope of our engagement did not include tests to determine whether control objectives not listed in section III were achieved; accordingly, we express no opinion on the achievement of control objectives not listed in section III.


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

The description of controls at CS is as of April 30, 2005, and the information about tests of the operating effectiveness of specific controls covers the period from October 1, 2004 to April 30, 2005. Any projection of such information to the future is subject to the risk

that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at CS 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 describing CS's transformation plans, as well as plans to modify service continuity plans, is presented by CS to provide additional information and is not part of CS's description of controls that may be relevant to a user organization's internal control. Such information 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.

By direction of the Deputy Inspector General for Auditing:

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

---

## **Section II: Information Provided by DISA**

---

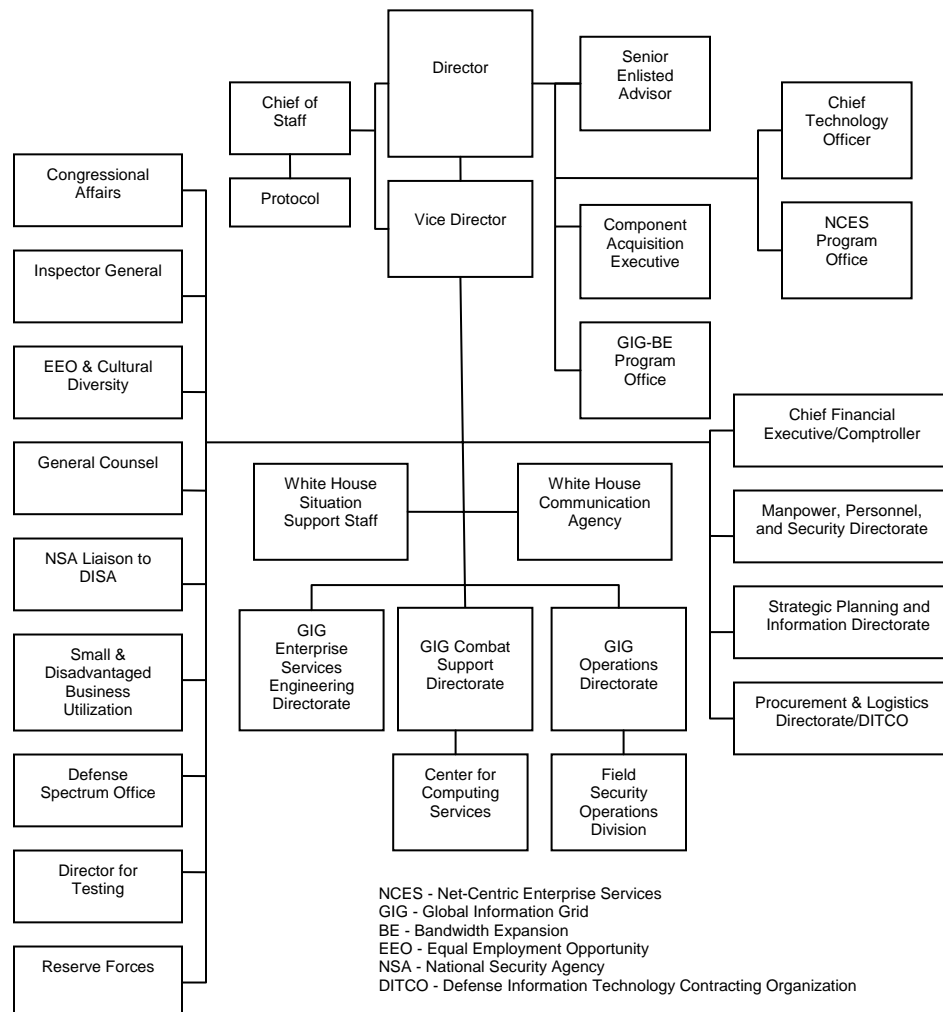


## A. Overview of Operations

### 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 solutions for the nation's warfighters and all those who support them in the defense of the nation. The core services are Acquisition, CS<sup>1</sup>, 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**



<sup>1</sup> Previously called Computing Services Directorate (CSD)

This report focuses on CS, under the GIG Combat Support Directorate. The FSO, under the GIG Operations Directorate, and other DISA organizations that support the CS are included only as they support the CS.

### **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 utilizing more than 40 mainframes and 3,000 servers. The supported applications: 1) provide command and control of warfighting forces, 2) facilitate mobility of the warfighters through maintenance of the airlifter and tanker fleets, 3) provide warfighter 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 utilizes 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 via utility contracts, enables DISA to provide the availability and surge capabilities that customers require.

CS offers computing services on both DISA-owned and customer-owned platforms. Computing services include computer operations, data storage, systems administration, security management, capacity management, system engineering, web and portal hosting, architectural development, and performance monitoring. Computing services are provided by a highly skilled workforce and performed in state-of-the-art computing facilities strategically located throughout the continental United States; 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.

**Headquarters.** The primary headquarters is located in Falls Church, Virginia. There are other headquarters elements located in Chambersburg, Denver, Dayton, and Pensacola, Florida<sup>2</sup>. There is 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 provides budgeting, resource management, manpower, personnel, training, business proposals, and Service Level Agreements. There are three primary elements: CS Headquarters, the Blue Ridge Center located in Chambersburg, and the Rocky Mountain Center located in Denver.

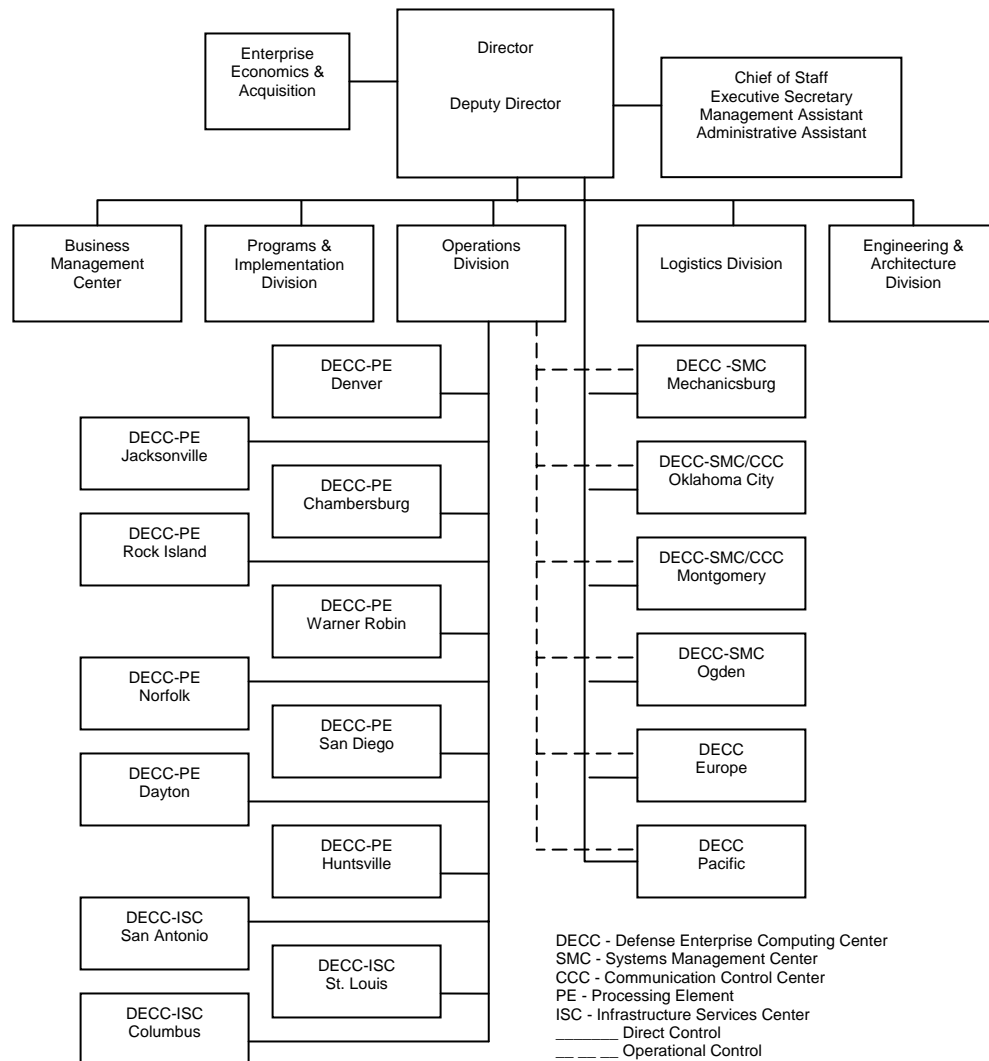
**Programs & Implementation Division.** The Programs & Implementation Division manages and directs assigned programs for CS. Programs include the migration

---

<sup>2</sup> The office in Pensacola provides financial services and technical support and coordinates all transactions between the Business Management Centers and Defense Finance and Accounting Service.

of legacy systems to standard systems, 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 System 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. This division has elements located at Falls Church and Denver.

**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. This division provides matrixed, cost-effective, integrated life cycle logistics and acquisition support services to CS. This division has offices in Chambersburg, Denver, and Dayton. 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.
- 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 in the Continental United States are divided into the following functional designations.

- 1) **System Management Centers (SMCs).** The primary responsibility of each SMC is systems management and customer support functions for the mainframe and server computing environments. The SMCs are located in Mechanicsburg, Montgomery, Ogden, and Oklahoma City.
- 2) **Infrastructure Services Centers (ISCs).** The ISCs perform system management for specialized fielding efforts from CS customers. The ISCs are located at Columbus and San Antonio.
- 3) **Processing Elements (PEs).** Facility management, hardware support, physical security, touch labor for communication devices, and touch labor for media management are the primary responsibilities for each PE. The PEs are located in Chambersburg, Dayton, Denver, Huntsville, Jacksonville, Norfolk, Rock Island, San Diego, and Warner Robins.

- 4) **Legacy DECC.** As a Legacy DECC, St. Louis has retained limited mainframe management and customer support functions. Until further optimization is completed, DECC St. Louis will have both SMC and PE responsibilities.

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

### **Information Assurance Support**

Almost all of the DISA elements interact with CS to some degree. The following DISA elements have the greatest IA interaction with CS.

**Chief Information Officer (CIO).** The CIO provides staff support in accomplishing Information Resources Management duties, mandated by the Clinger-Cohen Act. The CIO develops Information Resources Management and 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 Designated Approving Authority (DAA) for DISA owned and operated internal IT enclaves and networks. The CIO manages the agency-wide programs for Privacy Act and records management, and manages implementation of the DISA Electronic Business and Electronic Commerce.

**Field Security Operations.** The mission of FSO is to provide information systems, network security products, and direct funding and reimbursable services throughout DoD, including the combatant commands, the Services, and Defense agencies. The FSO supports the National Command Authority, combatant commanders, Joint Task Force 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 DAA. The FSO:

- develops, implements, and maintains security guidance and processes;
- conducts full scope security reviews and provides assistance to combatant commands, Directorates, Office of the Secretary of Defense, and DISA;
- provides certification and accreditation support;
- provides security training, security training products, and system administrator (SA) certification;
- implements security architecture and IA Tools;
- provides specialized security database support;
- provides security staff support to DISA Global Operations and CS;
- provides Regional Computer Emergency Response Team support; and
- provides Information Assurance Representatives to combatant commands.

In addition, FSO provides the following support to CS;

- serves as Information Assurance Manager (IAM) and provides guidance and advice to the Director of CS, his staff, and personnel on IA, communications, and emanation security;
- serves as the Security Manager (SM) and provides guidance and advice to the Director of CS, his staff, and personnel on physical, industrial, personnel, and information security and security management;
- provides technical support on IA to the CS Engineering and Architecture, Programs and Implementation, and Operations Divisions;
- develops IA and traditional security solutions for the Business Management Center for the development of business proposals;
- develops and maintains IA and traditional security policies and procedures for CS;
- prepares and maintains PE Security Plans and Security Standard Operating Procedures;
- develops, prepares, and maintains the System Security Authorization Agreement documents for the ISCs and PEs;
- provides advice to the IA staff of the SMCs on the preparation of their respective System Security Authorization Agreements; and
- prepares Security Technical Implementation Guides (STIGs) applicable to all DECCs.

## **B. Overview of Control Environment**

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

CS has the responsibility of providing core services and meeting the CS customer expectations through professional and consistent operations services and standard implementation of proven industry best practices. CS is responsible for continual refinement and analysis of operations performance metrics and practices to identify and implement opportunities for improvement in the execution of core operations services 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 OMB Circular A-130 requirements for a security program through DoD Instruction 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP),” December 30, 1997, and other DoD policies. DISA Instruction 630-230-19, “Automated Data Processing Information Systems Security Program,” 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 DAA. The DITSCAP and resultant Certification and Accreditation program are major components of DISA's security review program.

**Security Control Program at the DECCs.** The DISA Computing Services Security Handbook Version 3, Change 1, December 2000; the Information Assurance Vulnerability Alert Handbook; and the STIGs, primarily covers the DoD, Federal (OMB), 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 IAM.** The CS IAM provides guidance and advice to CS on IA, communications, and emanation security. This position is located within the FSO, but is matrixed to CS. The CS IAM reports to the Chief of Operations on security matters. In those cases where there is a disagreement relating to security, the CS IAM can go directly to the Deputy Director or Director of CS.

**CS 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 is matrixed to CS. The CS SM reports to the Chief of Operations on security matters. In those cases where there is a disagreement relating to security, the CS SM can go directly to the Deputy Director or Director of CS.

**Site IAM.** IAMs at the sites report to the Deputy Director or Director of the site. The IAM responsibilities are as follows:

- develop and maintain an organization or DoD information system-level IA program that identifies IA architecture, requirements, objectives and policies; personnel; and processes and procedures;
- ensure that information ownership responsibilities are established for each DoD information system, to include accountability, access approvals, and special handling requirements;
- ensure the development and maintenance of IA certification documentation according to DoD Instruction 5200.40, by reviewing and endorsing such documentation, and recommending action to the DAA;
- maintain a repository for all IA certification and accreditation documentation and modifications;
- ensure that Information Assurance Officers (IAOs) are appointed in writing, as required, and provide oversight to ensure that they are following established IA policies and procedures. In addition to meeting all access requirements specified in DoD Directive 8500.1, all newly appointed IAOs shall be U.S. citizens. Foreign nationals who are direct or indirect hires and are currently appointed as IAOs may continue in these positions provided they

satisfy the provisions of DoD Directive 8500.1, are under the supervision of an IAM who is a U.S. citizen; and are approved in writing by the DAA. When circumstances warrant, a single individual who is a U.S. citizen may fill both the IAM and the Information Assurance Officer (IAO) roles;

- ensure that all IAOs and privileged users receive the necessary technical and IA training, education, and certification to carry out their IA duties;
- ensure that compliance monitoring occurs, and review the results of such monitoring;
- ensure that IA inspections, tests, and reviews are coordinated;
- ensure that all IA management review items are tracked and reported;
- ensure that incidents are properly reported to the DAA and the DoD reporting chain, as required, and responses to IA-related alerts are coordinated; and
- act as the primary IA technical advisor to the DAA and formally notify the DAA of any changes impacting the DoD information system's IA posture.

**Site IAO.** IAOs at the sites report to the IAMs of the site. The IAO responsibilities are as follows:

- assist the IAM in meeting the duties and responsibilities outlined above;
- ensure that all users have the requisite security clearances and supervisory need-to-know authorization, and are aware of their IA responsibilities before being granted access to any DoD information system;
- initiate protective or corrective measures, in coordination with the IAM, when an IA incident or vulnerability is discovered;
- ensure that IA and IA-enabled software, hardware, and firmware comply with appropriate security configuration guidelines;
- ensure that DoD information system recovery processes are monitored and that IA features and procedures are properly restored;
- ensure that all DoD information system IA-related documentation is current and accessible to properly authorized individuals; and
- implement and enforce all DoD information system IA policies and procedures, as defined by its security certification and accreditation documentation.

### **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 SRR and the vulnerability scan used to determine the effectiveness of the network, systems, physical, personnel, information, and industrial security procedural countermeasures. These can be conducted by the FSO or as self-assessments performed by site personnel. Environmental and facility reviews conducted by CS Facility Engineers are used to determine the effectiveness of facility and environmental countermeasures. Various Federal Emergency Management Agency 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 DISA DAA (the DISA CIO). A complete formal review and documented risk assessment is only conducted every three years<sup>3</sup>.

**Mission Assurance Category.** The mission assurance category (MAC) reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighter combat mission. MACs are the basis for determining availability and integrity control requirements. DoD has three defined MACs.

- **MAC I.** Systems handling information that is vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.
- **MAC II.** Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance.
- **MAC III.** Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

---

<sup>3</sup> As a result of the transformation, most of the formal risk assessments will need to be updated to reflect the new environment.

## **Compliance Validation**

DISA compliance validation is conducted both externally by the FSO and within CS using automated scripts and the IA connection approval process. 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 which provide an unauthorized person or software immediate access into a system, gains privileged access, bypasses a firewall, or results in a denial of service.
- **Finding Category II.** Any vulnerability that provides information that has a high potential of giving access to an unauthorized person, or provides an unauthorized person the means to circumvent security controls.
- **Finding Category III.** Any vulnerability that provides information that potentially could lead to an unauthorized access.
- **Finding Category IV.** Any vulnerability that is all other possibilities that contributes to degraded security.

**External Compliance Validation.** The external compliance validation is conducted by the FSO. Because of the number and size of the sites, a complete review of each site cannot be made on an annual basis. The complete review is conducted during a three-year cycle to coincide with the formal accreditation cycle. The number of FSO visits is dependent on reviewing thirty-three percent of each site's assets on an annual basis. Per DITSCAP, accreditation decisions are made for a maximum of a three-year period. Annual reviews conducted by the FSO are known as Information Assurance Readiness Reviews. The Information Assurance Readiness Review includes a review of procedures, documentation, SRRs, and a vulnerability or penetration scan. All Information Assurance Readiness 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).

**Traditional SRR.** The traditional SRR determines whether policies and procedures on physical, information, personnel, industrial, communications, and emanations 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 STIGs.

**Vulnerability Scans.** The Vulnerability Assessment Process utilizes a commercial automated scanning tool, Internet Security Scan, that checks for known or demonstrated vulnerabilities. The scan is a two-step process. The first step is external to the perimeter of the enclave and determines the robustness of perimeter defenses. The second step is internal of 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. Where 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 utilizes 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 as the results of the FSO SRR scripts and checklists, and at least 90-95 percent compliance<sup>4</sup> 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 PE's 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 SSO Montgomery. The two databases do not share information at this time.

**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. 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 concurrence decision to the DISA approving authority.

The timeframe for correcting findings is 5 days or immediately for Category I, 180 days for Category II, and 270 days for Category III and IV vulnerabilities. The CS IAM notifies the responsible site IAM of any concerns and assets that are not in compliance

---

<sup>4</sup> The percentage varies based on the technology.



within allotted timeframes. The status of open Category I findings and findings that are not in compliance within the allotted timeframes are briefed to the Director, CS and primary CS staff<sup>5</sup> on a weekly basis.

**Vulnerability Compliance Tracking System database.** The Vulnerability Compliance Tracking System database tracks DISA's acknowledgement and compliance with the DoD Information Assurance Vulnerability Management<sup>6</sup> program. 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 alert by email. 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 and assets that are not in compliance within seven working days of the compliance date. The status of compliance is briefed to the Director of CS and primary staff on a weekly basis. The CS IAM also reviews requests for extensions to compliance dates and recommends a concurrence or non-concurrence 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 Database by the end of 2005. Automated SRR scripts are limited in that they cannot perform the manual checks of the STIGs. Automated SRR scripts only test the configuration settings of the hardware and software associated with the IT. Operating systems 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.

---

<sup>5</sup> Deputy Director, Chief of Staff, and the Division Chiefs for Business Management Center, Programs and Implementation, Engineering and Architecture, Operations, and Logistics.

<sup>6</sup> Includes alerts, bulletins, and advisories.

## **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 IDS, monitored by Global Network Security Center, is known as the Joint Intrusion Detection System. The Center monitors all Joint Intrusion Detection Systems on the GIG within the continental United States. There are various other centers located around the world and all centers feed into a DoD Global Network Center Network Defense. This concept can identify any information threat on an isolated, regional, or global basis. The Global Network Security Center notifies any element, to include CS, of any type of potential unauthorized attack or access. The Global Network Security Center 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 a network IDS. The security staff located in the CCCs develops the security profiles for the enclave perimeter router, perimeter firewall and perimeter network IDSs and monitor their respective reports and audit logs for unauthorized access or activities. This is for the entire continental United States-based CS network. The security staffs located at DECCs Europe and Pacific perform the same tasks locally for their respective enclave perimeter devices. Suspected incidents are investigated in concert with trusted agents from the customer base or data owners to determine the legitimacy of the incidents. If the suspected incident cannot be validated as authorized, they are reported to the Computing Services Cell within the DISA Network Operation Center and to the Global Network Security Center. The Global Network Security 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 weekly as a minimum 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, and identifies unauthorized privilege, or user-level action is identified, the action is reported to the Global Network Security 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 via 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 Office located at DISA Headquarters. The DISA Security Office issues requests for additional information, intent to deny or revoke, and actual revocations of security clearances or favorable investigations.

### **Environmental Controls**

The Facilities Engineering Branch, a CS Headquarters organization in Denver establishes facility standards for the DECCs on electrical distribution, uninterrupted power supply, fire detection and 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 located 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.

- Computer facilities have true floor-to-ceiling walls or alarms that dispatch a response team.
- Limited entrance and exit doors equipped with automated systems that require an access card and personal identification number to gain entry.
- Emergency exits are equipped with panic release bars that have a ½-inch deadbolt throw. Emergency exits do not have external opening devices.

- Doors and windows are equipped with intrusion detection systems that dispatch a response team.
- Doors are constructed of metal, solid wood, or glass. Door hinges are protected from removal by set screws, pins, or spot welds.
- Personnel authorized unescorted access are listed on access rosters.
- Visitors are required to sign into and out of the facility; and those that do not possess the required clearance must obtain unescorted badges and be escorted at all times while in the facility.
- Walls inside the building that are external to computing areas have signs posted identifying the area as a “Restricted Area.”

**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 General Services Administration (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 open 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 systems.

The Federal Information Processing Standards Publication 140-2 compliant encryption is used to protect the transmission of unclassified information, when required by the customer in the Service Level Agreement.

All computing areas that process classified information must be 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 be

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.

### **Industrial Security Controls**

Contracts must address security requirements. The contract should identify:

- the requirement for IT level and the personnel security investigation;
- the requirement for the contractor to provide visit request information for all contractor personnel that need to visit a government location;
- the requirement to comply with all security policies and procedures at government locations;
- the configuration requirement for contractor-provided equipment that will be connected to government networks and enclaves, if no government-furnished equipment is provided; and
- the requirement for a DD Form 254, for contracts that require access to classified information, that outlines the required level of security clearance, where classified information can be accessed, and any special instructions.

## **C. Information and Communication**

### **Information Systems Overview**

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

CS customer support demands include multiple classifications of secure environments, multi-vendor UNIX environments, Intel-based server environments, IBM and Unisys mainframe environments, multiple commercial database environments, commercial off-the-shelf 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 electronic mail messages to communicate time-sensitive messages and information. The Director of CS holds a

weekly staff meeting with all CS Division Chiefs. All site Chiefs also hold periodic staff meetings as appropriate. Every employee within CS has a written position description, and every position description includes details of what responsibilities are required of the individual.

The CS Business Management Center is responsible for Headquarters level customer relations and acts as the face to the customer.

Each operating site within CS maintains detailed records of problems reported by customer and problems or incidents noted during processing and monitor such items until they are resolved. The 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.

## **D. Control Objectives and Related Control Activities**

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

## **E. User Control Considerations**

### **Computing Services User Controls**

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

CS has established the following user controls for the computing environment.

- Each user has individual user identification for all platforms.
- Each user has individual user password authentication for open-system servers.
- Each user has individual user identification, password, and secure-identification for IBM mainframes.
- All privileged users should use the client-based Virtual Private Network or the Out-of-Band Network. Where there is an exception, privileged users must use encryption-protected access method (i.e. Secure Socket Layer or Secured Shell)
- All system access, by human or machine, requires DD Form 2875 (System Authorization Access Request).

- All users must acknowledge their responsibility for the user identifications and passwords.
- Each supervisor must acknowledge his subordinates' user requirement and IT level.
- The data owner or his designated representatives must acknowledge access for the data user.
- The SM must validate the user's security investigation and security clearance.
- Each user must attend initial and periodic IA awareness training.
- The SAs have passed the required security certification testing as a Level I, II or III as appropriate.
- The user systems will time out after 15 minutes if not in use.
- Lock-out of user identification and password after three incorrect log-on attempts.

### **Customer User Controls**

Customers are expected to have the following general user controls, at a minimum, built into their applications. The specific user controls are outlined in the Service Level Agreements.

- Individual user identification.
- Individual user password or Public Key Infrastructure authentication.

### **Service Level Agreements**

A service level agreement is a contract between a service agency and a customer agency that defines the parameters of the services. The Service Level Agreement defines the services to be delivered, problem management, and customer duties and responsibilities. The Service Level Agreements outline, at a minimum, the responsibilities over system access, security controls, data disposition and sharing, data encryption, and data backup for both CS and the customers.





---

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

---



## Entity-wide Security Program

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
<b>Control Objective:</b> <b>SP-1: Controls provide reasonable assurance that security risks are periodically assessed.</b>		
<p><b>Periodically assess security risks against federal requirements.</b></p> <p>A formal risk assessment is developed for each site and conducted once every 3 years. Formal risk assessments are updated annually based on annual reviews. The results of the traditional SRRs, technical SRRs, Internet Security Scans, Information Assurance Vulnerability Management, and the effectiveness of implemented countermeasures are used to determine the residual risk.</p> <p>Final risk determinations and related management approvals are documented and maintained on file.</p>	<p>Inspected policies and procedures for performing risk assessments and determined these policies and procedures were in place. Inquired of CS personnel to determine whether the policies and procedures were being followed. Inspected the most recent risk assessments to determine whether they were performed in accordance with the policies and were approved by management.</p> <p>Inquired of the objectivity of the personnel who performed the risk assessments to determine they were independent of the systems that were reviewed.</p>	<p>Risk assessments at two out of six sites did not conform to the FSO Risk Analysis Guide.</p> <p>No relevant exceptions noted.</p>

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p><b>Control Objective:</b>  <b>SP-2: Controls provide reasonable assurance that an entity-wide security program plan is documented, approved, and kept current.</b></p>		
<p><b>A security plan is documented and approved.</b></p> <p>The security plan is documented and addresses topics prescribed in OMB Circular A-130, Security of Federal Automated Information Resources. The security plan is validated for completeness and applicability during the FSO's Traditional SRR.</p> <p>The SMCs security plan is developed by the site SM or IAM and signed by the senior official on site.</p>	<p>Inspected site security plans to determine whether the following had been addressed:</p> <ul style="list-style-type: none"> <li>• management review of the plan on a regular basis, at least annually, to evaluate existing policies and processes and to provide consistency and support for the goal of uninterrupted operations;</li> <li>• management's approval of the security plan in writing; and</li> <li>• guidance related to security plans for general support systems, as outlined in OMB Circular No. A-130 Appendix III.</li> </ul>	<p>One out of six sites did not have a current security plan that was documented and approved.</p>
<p><b>The security plan is kept current.</b></p> <p>The security plan is reviewed annually and updated annually or as necessary.</p>	<p>Inspected the security plan to evaluate:</p> <ul style="list-style-type: none"> <li>• factors that caused the plan to be updated;</li> <li>• plan was current;</li> <li>• supporting documentation existed for any changes during the last year;</li> <li>• documentation existed to depict how systems and applications were interconnected, including connection rules and requirements;</li> <li>• documentation existed to sufficiently assess the impacts of any changes made; and</li> </ul>	<p>For two out of six sites, the security plans did not incorporate current guidance provided by DoD Instruction 8500.2 and OMB Circular A-130 Appendix III.</p>

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> <li>plans covered the current topics outlined in OMB Circular A-130 Appendix III, and DoD Instruction 8500.2.</li> </ul>	
<b><i>Control Objective:</i></b> <b>SP-3: Controls provide reasonable assurance that a security management structure is established and security responsibilities are clearly assigned.</b>		
<b>A security management structure has been established.</b>  The CS Security Handbook defines the responsibilities of individuals who comprise the security management staff.	Inquired of CS management to determine whether: <ul style="list-style-type: none"> <li>a security staff was designated for each site; and</li> <li>clear assignments of information security responsibilities that addressed information security roles, training, and security clearances existed.</li> </ul>	No relevant exceptions noted.
<b>Information security responsibilities are clearly assigned.</b>  The roles and responsibilities of the IAM, IAO, and SM are outlined in appointment orders.	Inquired of CS management whether security responsibilities had been clearly assigned to the following: <ul style="list-style-type: none"> <li>information resource owners and users,</li> <li>information resources management and data processing personnel,</li> <li>senior management, and</li> <li>security administrators.</li> </ul>	No relevant exceptions noted.

<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
<p><b>Owners and users are aware of security policies.</b></p> <p>CS personnel must take security awareness training, workplace violence training, and antiterrorism training before gaining access to any system. Initial security awareness training is provided to all users. Training completion is recorded.</p> <p>Posters are utilized throughout the CS facilities to increase security awareness on various security-related topics, such as viruses, freeware or shareware, and unique passwords.</p> <p>CS employees are required to sign non-disclosure agreement forms to evidence their understanding and acceptance of confidential information disclosure restrictions and requirements.</p>	<p>Inquired of CS management about the existence of an ongoing security awareness program for current employees and an introductory program for new employees.</p> <p>Inspected other means used by CS to promote security awareness.</p> <p>Inspected employees' non-disclosure agreement forms to evidence their understanding and acceptance of confidential information disclosure restrictions and requirements.</p>	<p>Three out of six sites did not have an effective security awareness program that provided guidance to users regarding the importance of security.</p> <p>No relevant exceptions noted.</p> <p>Two out of six sites did not have effective procedures implemented to determine that employees and contractors complete a non-disclosure agreement form to evidence their understanding and acceptance of confidential information disclosure restrictions and requirements.</p>
<p><b>An incident response capability has been fully implemented.</b></p> <p>The CS Security Handbook provides guidance on handling incidents, incident reporting structure, and prioritization of incidents that are consistent with attributes suggested by DoD Instruction 8500.2.</p>	<p>Inquired of site personnel regarding their familiarity with their specific responsibilities for intrusion detection and incident response.</p>	<p>Personnel at four out of six sites were not familiar with their responsibilities for intrusion detection and incident response.</p>

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p><b>Control Objective:</b>  <b>SP-4: Controls provide reasonable assurance that effective security-related personnel policies have been implemented.</b></p>		
<p><b>Hiring, transfer, termination, and performance policies address security.</b></p> <p>The CS Security Handbook prescribes guidelines addressing personnel security controls and position sensitivity designations for employees and contractors, documenting and updating designations, investigation and reinvestigation requirements, adjudication, clearance procedures, and termination processing.</p> <p>Personnel security checks to determine that a valid and current personnel security investigation has been conducted for each person at the site based on the individual's duties and tasks.</p> <p>Termination requires debriefing and revoking of all access. Termination debriefing must be signed and maintained.</p>	<p>Inspected the hiring policies and procedures for employees and for contractors, including reviewing the process for performing background investigations and contacting references for new hires.</p> <p>Inspected policies and procedures in place for performing reinvestigations of current employees and contractors.</p> <p>Inspected CS policies and procedures in place for individuals departing CS, or where systems access was no longer required.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>Three out of five sites did not implement formal policies for debriefing and removing all access.</p>
<p><b>Employees have adequate training and expertise.</b></p> <p>Training and certification requirements for users and SAs are established by DoD and DISA policies.</p>	<p>Inquired of CS management whether employees were receiving appropriate training and had the necessary skills to perform assigned job functions.</p>	<p>Personnel at three out of five sites did not receive appropriate training to perform their duties.</p>



<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
The CS Security Handbook outlines several different certification courses that SAs and security management should take depending on the designated level	Inspected documentation regarding training programs to determine whether employee training and professional development activities were documented and monitored.	Three out of five sites did not document employee training and professional development activities.
<b><i>Control objective:</i></b> <b>SP-5: Controls provide reasonable assurance that security program effectiveness is monitored and changes are made as needed.</b>		
<p><b>Management periodically assesses the appropriateness of security policies and compliance with them and ensures that corrective actions are effectively implemented.</b></p> <p>The FSO performs SRRs as a part of its IA review and certification and accreditation process. The FSO also conduct annual reviews to assess the appropriateness of the security policies and compliance with them. CS and FSO have visibility over all identified vulnerabilities.</p> <p>Automated scripts are performed on a weekly basis for servers at the four main SMCs. The sites also perform vulnerability assessments.</p> <p>New systems are reviewed for compliance with DoD and STIG policy prior to connection to the network.</p>	<p>Inquired of CS management whether a comprehensive vulnerability management process was in place to address:</p> <ul style="list-style-type: none"> <li>• systematic identification and mitigation of software and hardware vulnerabilities,</li> <li>• independent validation of mitigation through inspection and automated vulnerability assessment,</li> <li>• acquisition of vulnerability assessment tools, and</li> <li>• deployment of trained personnel.</li> </ul> <p>Inquired of CS management whether regular internal and external assessments were conducted.</p> <p>Inspected whether new systems and major upgrades were tested prior to connection to the network and authorized.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>For one out of five sites, new systems and major upgrades were not fully tested and authorized prior to connection to the network.</p>

## Access Control

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
<b><i>Control Objective:</i></b> <b>AC-1: Controls provide reasonable assurance that information resources are classified according to their criticality and sensitivity.</b>		
<b>Resource classifications and related criteria have been established.</b>  CS has defined the criticality of its assets and the policies to the MAC II sensitive level.	Inspected the policies and procedures that CS used to develop and establish data and resource classification rankings for adequacy and effectiveness.	No relevant exceptions noted.
<b>Owners have classified resources.</b>  CS has classified the criticality of its assets.  CS customers communicate classification levels to CS for their applications.	Inquired whether assets had been classified, and the classifications were documented and current.  Inquired of site IAMs how customers communicated classification levels for their application that were in accordance with the specific risk assessment results.	No relevant exceptions noted.  No relevant exceptions noted.

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p><b>Control Objective:</b>  <b>AC-2: Controls provide reasonable assurance that a current list of authorized users and their respective access rights are maintained.</b></p> <p><b>Design Weakness:</b>            CS does not have control procedures in place to ensure resource owners have identified authorized users and their respective access rights. Specifically, control procedures are needed to ensure the following: (a) access rights associated with role-based user accounts are fully established across CS, and (b) account maintenance practices and procedures have been fully implemented across CS platforms.</p>		
<p><b>Resource owners have identified authorized users and their authorized access rights.</b></p> <p>The CS Security Handbook details the process for granting access to system resources.</p> <p>System access is role-based, which depends on tasks and functions.</p> <p>IAM maintains a list of all approved privileged users for operating systems, networks, databases, and web administrators. This includes those privileged users within or outside of CS.</p> <p>Each user identification issued is evidenced by a DD Form 2875 (or its predecessor DISA Form 41) or a local form that has incorporated all the requirements of the DD</p>	<p>Inspected procedures that CS followed to grant access to its systems.</p> <p>Inspected access rights associated with user accounts to determine if they had been established in accordance with a role-based access scheme that organizes system and network access rights into roles.</p> <p>Inquired of management to determine that sites have IAMs, and determined whether the IAMs track privileged role assignments.</p> <p>Inspected policies and procedures for granting operating system access, including required approval by information owners.</p> <p>Inquired to determine whether a comprehensive account management process existed to:</p> <ul style="list-style-type: none"> <li>allow only authorized users to gain</li> </ul>	<p>No relevant exceptions noted.</p> <p>Refer to the design weakness noted above, item (a).</p> <p>IAM at four out of six sites did not track privileged role assignments.</p> <p>No relevant exceptions noted.</p> <p>Refer to the design weakness noted above, item (b).</p>

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>Form 2875. DD Form 2875, System Access Authorization Request, requires approval from the user's supervisor, data owner, and validation of user personnel security investigation based on access requested.</p> <p>Periodic revalidation of system users is conducted to identify accounts and user accesses that are no longer needed.</p>	<p>access to workstations, applications, and networks; and</p> <ul style="list-style-type: none"> <li>deactivate individual accounts designated as deactivated, suspended, or terminated.</li> </ul> <p>Inquired of management regarding the process to determine that access authorizations were in accordance with DoD personnel security policies and security criteria (i.e. background investigation requirements outlined in DoD Regulation 5200.2-R).</p> <p>Inquired whether information assurance managers were performing periodic revalidations of system users.</p>	<p>No relevant exceptions noted.</p> <p>Four out of five sites had no processes for conducting periodic revalidations of system users.</p>
<p><b>Emergency and temporary access authorization is controlled.</b></p> <p>Emergency and temporary access authorizations are:</p> <ul style="list-style-type: none"> <li>documented and maintained on file,</li> <li>approved by appropriate management,</li> <li>securely communicated to the IAM, and</li> <li>terminated after a predetermined period.</li> </ul>	<p>Inquired whether CS had established policies and procedures for the creation and maintenance of emergency and temporary access to CS owned or administered systems.</p> <p>Inspected a listing of emergency and temporary user access requests to determine whether:</p> <ul style="list-style-type: none"> <li>a record of such access was maintained,</li> <li>management approved the access,</li> </ul>	<p>One out of six sites did not have policies and procedures in place for the creation and maintenance of emergency IDs.</p> <p>Two out of six sites did not maintain a record of emergency and temporary user access requests.</p>

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> <li>and</li> <li>access was terminated in a specific period of time.</li> </ul>	
<p><b>Owners determine disposition and sharing of data.</b></p> <p>The Support Agreement portion of the Service Level Agreements defines the data disposition and data sharing process.</p>	<p>Determine whether Service Level Agreements addressed file sharing and IA roles and responsibilities for the acquisition or outsourcing of IT services.</p>	<p>No relevant exceptions noted.</p>
<p><b><i>Control Objective:</i></b>  <b>AC-3: Controls provide reasonable assurance that physical and logical controls to prevent or detect unauthorized access are fully established and access to and use of system software is monitored.</b></p> <p><b><i>Design Weakness:</i></b>  CS does not completely have DoD required logical control procedures in place to fully ensure passwords, tokens, or other devices are used to identify and authenticate users; access paths are identified and access authorizations are appropriately limited; policies and techniques have been implemented for using and monitoring the use of system utilities, as well as for investigating and resolving inappropriate or unusual activity; telecommunications are secured; and cryptographic tools are used in a secure fashion. Specifically, control procedures are needed to ensure the following: (a) all relevant password policies and procedures are fully implemented at CS sites; (b) password settings are fully in compliance with the CS policies; (c) vendor supplied passwords are always removed or controlled once software has been installed; (d) SAs' access is consistent with the controls required by DoD over IA; (e) permissions to access devices, directories, files and registry settings have been fully established to comply with the STIGs; (f) operating system parameters are configured to maintain integrity of the security software and application controls; (g) system software monitoring utilities are installed; (h) system software information is logged and reviewed; (i) policies and procedures have been fully established to control and monitor internal and remote access; (j) configuration and security settings are fully in compliance with STIGs for network devices; (k) warning banners are displayed across all platforms hosted by CS; (l) policies and procedures are fully implemented for the use of cryptographic tools; and (m) devices are subject to an approved communications encryption method to perform remote management and file transfers.</p>		



<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
<p>The computer facility has:</p> <ul style="list-style-type: none"> <li>• true floor-to-ceiling walls,</li> <li>• solid entrance doors,</li> <li>• doors with hinges that prevent easy removal,</li> <li>• emergency doors free of devices on the outside and equipped with a panic bar release on the inside and a ½ inch deadbolt throw, and</li> <li>• doors with balanced magnetic switches.</li> </ul> <p>All CS site SMs must maintain and post an authorized access list inside of the computing facilities. Changes to the authorized access list can be made in pen and initialed by the SMs. The authorized access list must be updated on an annual basis.</p>	<p>Inspected access restrictions to the computer room to determine the existence of:</p> <ul style="list-style-type: none"> <li>• true floor-to-ceiling walls,</li> <li>• solid entrance doors,</li> <li>• doors with hinges that prevent easy removal,</li> <li>• emergency doors that were free of devices on the outside and equipped with a panic bar release on the inside and a ½ inch deadbolt throw,</li> <li>• doors with balanced magnetic switches, and</li> <li>• a process to control keys.</li> </ul> <p>Inspected a list of individuals having access to the sensitive areas to determine their authorizations.</p>	<p>Eight out of sixteen sites did not fully implement access restrictions to the computer room.</p> <p>Thirteen out of sixteen sites did not restrict access to sensitive areas to unauthorized individuals. However, access to CS facilities located on military or GSA installations was controlled by local military, DoD, or GSA police who performed routine patrols and random door checks.</p>
<p><b>Visitors are controlled.</b></p> <p>All visitors have a visit authorization request on file with the site SM.</p> <p>Visitors to the computing facilities that are not on the authorized access list must be signed in and out of the facility.</p>	<p>Inspected procedures for handling visitors to determine whether they:</p> <ul style="list-style-type: none"> <li>• were required to be escorted, and</li> <li>• had been cleared by the sponsor and security.</li> </ul> <p>Inquired to determine if there were procedures in place to control visitor access to the computer room.</p>	<p>No relevant exceptions noted.</p> <p>Eleven out of sixteen sites did not fully implement procedures to control visitor access to the computer room. However, all visitors who are not on the authorized</p>

<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
<p>CS personnel who do not have the appropriate security investigation or clearance and all non-CS personnel will be escorted at all times while in the computing facility.</p> <p>Entry codes are periodically changed.</p>	<p>Inspected policies for changing access codes (cipher locks) and obtained supporting documentation for these changes.</p>	<p>access list are signed in and out of the facility by guards who check identification.</p> <p>Eleven out of fourteen sites did not fully implement procedures for changing access codes.</p>
<p><b>Passwords, tokens, or other devices are used to identify and authenticate users.</b></p> <p>Password configuration requirements:</p> <ul style="list-style-type: none"> <li>• Minimum of 8 characters,</li> <li>• One lower-case character,</li> <li>• One upper-case character,</li> <li>• One number, and</li> <li>• One special character.</li> </ul> <p>Additionally,</p> <ul style="list-style-type: none"> <li>• Passwords changed every 90 days.</li> <li>• Password can only be changed once within 24 hours.</li> <li>• Password cannot be reused for 10 cycles.</li> <li>• Password cannot reuse any character more than once.</li> <li>• Passwords are encrypted in storage.</li> </ul> <p>Vendor-supplied default logons and passwords are disabled.</p>	<p>Inspected CS password policies to determine whether these policies and procedures met Federal, DoD, and DISA requirements.</p> <p>Inspected password settings to determine compliance with the policies.</p> <p>Inspected whether CS determines that all vendor supplied passwords were removed or controlled once the software has been installed.</p>	<p>Refer to the design weakness noted above, item (a).</p> <p>Refer to the design weakness noted above, item (b).</p> <p>Refer to the design weakness noted above, item (c).</p>



<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
<p>Passwords are subjected to software attacks as part of Internet Security Scanner scan and SRRs. Passwords are checked as part of the SRRs and self-assessments. Servers managed by the SMCs are being checked on a weekly basis with the automated scripts.</p>	<p>Inquired whether password were checked as part of the SRR process.</p> <p>Inspected whether password scanning tools were being executed on a weekly basis.</p>	<p>No relevant exceptions noted.</p> <p>For 16 of 49 Unix devices, the weekly password scan was disabled.</p>
<p><b>Access paths are identified and access authorizations appropriately limited.</b></p> <p>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.</p> <p>System software is configured in accordance with the STIGs.</p> <p>Access to data files, software programs and databases is controlled by the configuration setting as described in the STIGs.</p> <p>Network diagrams are developed and maintained to show potential access paths.</p> <p>The operating system and communications software are configured to prevent circumvention of security software controls and unauthorized access from all paths.</p>	<p>Inspected the topography diagram to determine whether an analysis of the logical access paths was performed whenever changes were made to CS owned or administered systems.</p> <p>Inspected to determine SAs’:</p> <ul style="list-style-type: none"> <li>• access granted met DoD IA controls;</li> <li>• access was consistent with their job responsibilities;</li> <li>• accounts designated as inactive, suspended, or terminated had been promptly deactivated;</li> <li>• access was reviewed frequently;</li> <li>• access was supported by a completed System Access Authorization Request on file; and</li> <li>• access was granted based on least-privilege access at the operating system level.</li> </ul> <p>Also, inspected access to platforms by attempting to gain access to the operating system and other system components.</p>	<p>No relevant exceptions noted.</p> <p>Refer to the design weakness noted above, item (d).</p>

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<p>Inspected configuration settings to determine whether access to the data files and software programs was in compliance with the STIGs.</p> <p>Inspected the operating system parameters to determine whether configurations:</p> <ul style="list-style-type: none"> <li>• maintain the integrity of the security software and application controls; and</li> <li>• allow access via approved paths to the operating system, kernel, system security software, and when applicable, application software.</li> </ul>	<p>Refer to the design weakness noted above, item (e).</p> <p>Refer to the design weakness noted above, item (f).</p>
<p><b>Policies and techniques have been implemented for using and monitoring use of system utilities and inappropriate or unusual activity is investigated and appropriate actions taken.</b></p> <p>Procedures are in place for monitoring, investigating and reporting inappropriate or unusual activity. The STIG outlines what activity is to be monitored and, within these guidelines, local policy determines the thresholds for what is considered inappropriate or unusual activities.</p> <p>System utilities are installed in accordance with policies and procedures for proper use of system utilities. These are documented in the STIGs, vendor documentation, and applicable users' manuals. Each site is</p>	<p>Inspected policies and procedures pertaining to monitoring, investigating, and reporting inappropriate and unusual activities on the use of system software utilities.</p> <p>Inspected whether system utilities, intended for monitoring inappropriate or unusual activity, were installed.</p>	<p>No relevant exceptions noted.</p> <p>Refer to the design weakness noted above, item (g).</p>

<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
<p>responsible for implementing these guidelines.</p> <p>The use of sensitive system utilities is logged and inappropriate or unusual activity is investigated.</p>	<p>Inspected the type of information being logged, the frequency of review and backup, and the sufficiency of data collected to detect operational or security abnormalities.</p>	<p>Refer to the design weakness noted above, item (h).</p>
<p><b>Telecommunications are secured.</b></p> <p>Telecommunications access is controlled by the managing CCC for the network devices, to include firewall and network IDSs, at all sites within continental United States for unclassified wide area network. For each site that had not yet “transformed,” the sites are responsible for the network devices. For those networks that have been transformed, only CCC personnel have access to those networks through the out-of-band virtual private network tunnel.</p> <p>Dial-in telephone numbers are not published and are periodically changed.</p>	<p>Inspected policies and procedures that had been established to control and monitor internal and remote access.</p> <p>Inspected settings for network devices to determine compliance with the STIGs.</p> <p>Inspected the warning banner when individuals log on to their computers and access the local area network or wide area network to determine whether all users were warned that they were entering a government information system, and were provided with appropriate privacy and security notices.</p> <p>Inquired if remote access numbers were changed periodically and not published in CS phone lists.</p>	<p>Refer to the design weakness noted above, item (i).</p> <p>Refer to the design weakness noted above, item (j).</p> <p>Refer to the design weakness noted above, item (k).</p> <p>No relevant exceptions noted.</p>

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p><b>Cryptographic tools are used in a secure fashion.</b></p> <p>When required by the customer, the Federal Information Publication Standards 140-2 compliant encryption is used for encryption of unclassified information.</p> <p>Encryption tools such as Virtual Private Network, Secure Socket Layer, Secure Shell, and Public Key Infrastructure are used where the data or the transmission of data needs to be protected.</p>	<p>Inspected policies and procedures outlining the use of cryptographic tools to encrypt stored sensitive information.</p> <p>Inspected devices to determine whether approved cryptography was used to encrypt stored sensitive information and inspected whether information in transit through a network was using approved cryptography when required.</p>	<p>Refer to the design weakness noted above, item (l).</p> <p>Refer to the design weakness noted above, item (m).</p>
<p><b>Sanitation of equipment and media prior to disposal or reuse.</b></p> <p>Sanitation of equipment and media prior to disposal or reuse are performed in accordance with DoD Regulation 5200.1-R, CS Security Handbook, and the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," dated June 4, 2001.</p>	<p>Inspected CS policies and procedures, and related documentation supporting the sanitation of equipment and media.</p>	<p>Two out of six sites did not fully comply with policies and procedures for sanitation of equipment.</p>

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p><b>Control Objective:</b>  <b>AC-4: Controls provide reasonable assurance that access is monitored, apparent security violations are investigated, and appropriate remedial action is taken.</b></p> <p><b>Design Weakness:</b>            CS does not have control procedures in place to fully ensure audit trails are maintained and actual or attempted unauthorized, unusual, or sensitive access is monitored. Specifically, control procedures are needed to ensure the following: (a) audit trails are monitored across all CS sites, and (b) devices have host-based intrusion detection systems fully deployed or implemented across CS sites.</p>		
<p><b>Audit trails are maintained.</b></p> <p>STIGs define audit trail requirements.</p> <p>For mainframe computers, three access programs (Resource Access Control Facility, Access Control Facility 2, and Top Secret) have the ability to conduct full audit and record audit records. The access program for Unisys mainframe also can conduct and record full audit records. For mid-tier systems, databases and web-based applications, audit capability is implemented if it does not impact performance and system storage devices overloads.</p> <p>Audit records are maintained for 1 year.</p>	<p>Inspected the audit trail monitoring, analysis, and reporting processes to determine that an automated audit trail capability is in place.</p> <p>Inquired of IAMs to determine whether they retained backups of audit records for one year.</p>	<p>Refer to the design weakness noted above, item (a).</p> <p>Three of four sites did not have procedures to retain backups of audit records for one year.</p>

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p><b>Actual or attempted unauthorized, unusual, or sensitive access is monitored.</b></p> <p>Suspicious access activity is investigated and appropriate action taken. The security staffs located in the SMCs, ISCs and CCCs monitor their respective reports and audit logs for unauthorized access or activities. 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 Global Network Security Center.</p>	<p>Inspected reports generated to track security violations on CS owned or administered systems to determine how questionable violations were documented and handled.</p> <p>Inspected network and host-based intrusion detection systems to determine they were deployed where required.</p>	<p>Three out of six sites did not fully comply with policies and procedures for handling security violations on CS owned or administered systems.</p> <p>Refer to the design weakness noted above, item (b).</p>

## Software Development and Change Control

<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
<b>Control Objective:</b> <b>CC-1: Controls provide reasonable assurance that processing features and program modifications are properly authorized.</b>		
<p><b>Authorizations for software modifications are documented and maintained.</b></p> <p>Configuration Control Board has been established to manage the configuration management process. The Configuration Control Board has the authority to approve or disapprove proposed changes to hardware, operating system, utility software, communications, and networks brought about by proposed application software changes.</p>	<p>Inquired of management the configuration management process to determine whether the configuration management process addresses:</p> <ul style="list-style-type: none"> <li>• documentation of configuration management roles and responsibilities,</li> <li>• the establishment of a Configuration Control Board,</li> <li>• a testing process to verify changes prior to implementation, and</li> <li>• a verification process to provide assurance that the configuration management process was working effectively.</li> </ul> <p>Inspected changes to applications or system software (updates or modifications) made for which CS had change control-related responsibilities to determine whether the changes were properly authorized and documented.</p>	<p>One of out six sites did not fully implement configuration management procedures.</p> <p>Six out of six sites did not always document configuration change requests, including authorizations.</p>
<p><b>Use of public domain and personal software is restricted.</b></p> <p>CS management has implemented policy that prohibits the usage of personal software on</p>	<p>Inquired of management regarding the policies and procedures restricting the use</p>	<p>One out of five sites did not fully implement policies and procedures</p>

<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
<p>the public domain.</p> <p>Users of CS resources use only software that is properly approved and accredited for CS use.</p>	<p>of personal and public domain software and instant messaging.</p> <p>Inspected CS procedures for enforcing policies that prohibit personal use of binary or machine executable public domain software, shareware, and freeware by inspecting computers or workstations to determine compliance.</p>	<p>restricting the use of personal and public domain software and instant messaging.</p> <p>Users at four out of five sites did not always use software that was properly approved or accredited.</p>
<p><b><i>Control Objective:</i></b>  <b>CC-2: Controls provide reasonable assurance that all new and revised software including system software are tested and controlled.</b></p>		
<p><b>Changes are controlled as software progresses through testing to final implementation.</b></p> <p>Procedures are in place for the testing, test analysis, test reporting, and approval for release to operational sites for all system software changes.</p> <p>For system software:</p> <ul style="list-style-type: none"> <li>• full integration testing is performed to ensure functionality;</li> <li>• performance and stress testing is performed, as required, to identify impacts on system performance; and</li> <li>• security testing is performed for each system software release. Based upon test results, actions are initiated to rectify identified software</li> </ul>	<p>Inspected policies and procedures for the installation, upgrade, and maintenance of system software.</p> <p>Inquired procedures for modifications to enterprise applications (or other applications for which CS had change control-related responsibilities), including patches, upgrades and new applications.</p> <p>Inquired of management regarding whether controls were adequate to prevent the implementation of unauthorized system software or changes to system software.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>Two out of six sites did not fully implement controls to prevent the implementation of unauthorized system software or changes to system software.</p>



<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
<p>deficiencies, performance impacts, and security problems.</p>	<p>Inspected the test plan standards that have been developed for all levels of testing to include:</p> <ul style="list-style-type: none"> <li>• definition of responsibilities for each party, including (users, system analysts, programmers, and quality control);</li> <li>• encompassing procedures for assessing IA and impact on accreditation; and</li> <li>• requirement for approval before proceeding to the next level of testing.</li> </ul> <p>Inspected if CS had separate environments for development, testing, and production.</p> <p>Inquired of management regarding who was responsible for moving changes between development, testing, and production environments.</p> <p>Inquired of management regarding how access is controlled between these environments (development, test, and production) for non-end users and inspected for compliance.</p> <p>Inspected the listing to determine whether CS programmers have access to the production environment, and whether end users have access to the development and test environments.</p>	<p>One out of six sites did not fully develop test plan standards for all levels of testing.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p> <p>CS programmers at one out of six sites had unauthorized access to the production environment.</p>

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<p>Inspected whether CS maintains an audit trail or log of identified system software changes and issues to determine that the log included:</p> <ul style="list-style-type: none"> <li>• date, time, and type of event;</li> <li>• user identification; and</li> <li>• problem description, assigned reviewer, and problem resolution.</li> </ul>	<p>Three out of six sites did not fully maintain audit trails or logs for system software changes.</p>
<p><b>Emergency changes are promptly tested and approved.</b></p> <p>Emergency change procedures are documented.</p> <p>Emergency changes are moved into production only after changes are tested and documented prior to final approval by the Configuration Control Board.</p>	<p>Inquired of management regarding the policies and procedures in place for emergency changes.</p> <p>Inspected the following for emergency changes:</p> <ul style="list-style-type: none"> <li>• emergency changes were recorded and approved by management;</li> <li>• normal change request forms and documentation were completed after the emergency change; and</li> <li>• independent review of changes was performed.</li> </ul>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>
<p><b>Control Objective:</b>  <b>CC-3: Controls provide reasonable assurance that software libraries are controlled.</b></p>		
<p><b>Access to program libraries is restricted.</b></p> <p>Source code is maintained in separate libraries.</p>	<p>Inquired of management to determine that source code for the most recent version was maintained in a separate library from</p>	<p>No relevant exceptions noted.</p>

<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
	<p>production code.</p> <p>Inspected the access control software rules to determine they were clearly defined.</p>	<p>No relevant exceptions noted.</p>
<p><b>Movement of programs and data among libraries is controlled.</b></p> <p>Verification and acceptance of software changes is documented and approved and movements are controlled.</p>	<p>Inspected policies and procedures for movement of program code between libraries.</p> <p>Inspected documentation maintained to track the movements or changes to determine they were approved.</p>	<p>Two out of four sites had incomplete procedures for movement of program code between libraries.</p> <p>Three out of five sites had incomplete documentation to support approvals for the movement of program and data among libraries.</p>

## Segregation of Duties

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
<b>Control Objective:</b> <b>SD-1: Controls provide reasonable assurance that incompatible duties are segregated and related policies are established.</b>		
<p><b>Incompatible duties have been identified and policies implemented to segregate these duties.</b></p> <p>CS Security Handbook describes the job responsibilities that are supplemented by local site policies. The job responsibilities are based on roles and responsibilities for department personnel. Service Level Agreements also describe the roles and responsibilities of CS personnel responsible for maintaining the customer platforms.</p>	<p>Inspected policies and procedures concerning employee responsibilities and segregation of duties, to address:</p> <ul style="list-style-type: none"> <li>• consistency with the current operating environment;</li> <li>• identification of sensitive functions and incompatible duties; and</li> <li>• understanding of management and information systems personnel's responsibilities about segregation of duties.</li> </ul> <p>Inspected the site's organization chart depicting information security functions and assigned personnel to determine if individuals were assigned incompatible roles.</p> <p>Reviewed site organization charts depicting information security functions and assigned personnel to determine whether</p> <ul style="list-style-type: none"> <li>• the chart reflected the current</li> </ul>	<p>Two out of six sites did not have policies and procedures addressing employee responsibilities and segregation of duties.</p> <p>One out of six sites did not have roles assigned based on appropriate segregation of duties.</p> <p>Two out of six sites did not have distinct system support responsibilities that were performed by different personnel.</p>

<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
	<p>organizational structure;</p> <ul style="list-style-type: none"> <li>• each function was staffed by a different individual; and</li> <li>• alternate or backup assignments had been made, if applicable,.</li> </ul> <p>Inquired of selected individuals to determine if they performed only their primary job functions and if secondary duties were performed, whether these duties created a segregation of duties issue.</p> <p>Inspected the activities of selected individuals to determine the nature and extent of compliance with applicable segregation of duties policies.</p> <p>Inspected to determine whether sites with limited resources to segregate duties had implemented compensating controls.</p>	<p>No relevant exceptions noted.</p> <p>Personnel at one out of six sites did not comply with applicable segregation of duties policies.</p> <p>One out of six sites did not implement appropriate controls over segregation of duties.</p>
<p><b>Job descriptions have been documented.</b></p> <p>All civilian personnel have position descriptions.</p>	<p>Inspected a sample of position descriptions in different organizational units to determine whether:</p> <ul style="list-style-type: none"> <li>• duties were clearly described,</li> <li>• position descriptions were current,</li> <li>• job descriptions reflected current responsibilities and duties, and</li> <li>• technical knowledge, skills, and abilities required for successful performance were included for technical positions.</li> </ul>	<p>One out of six sites did not have fully documented position descriptions for all civilian personnel.</p>

<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
<p><b>Employees understand their duties and responsibilities.</b></p> <p>Supervisors maintain copies of position descriptions, and ensure that they correctly identify the task and functions required by the position.</p> <p>Supervisors at all levels develop and maintain a performance plan for each individual and ensure that the plan requires the performance based on the position description.</p>	<p>Inquired of personnel whether their position descriptions match their understanding of their duties and responsibilities and whether additional duties were undertaken that were not listed in their position descriptions or performance plan.</p> <p>Inquired of management personnel in key operating and programming positions to determine if responsibilities for restricting access by position descriptions were clearly defined, understood, and followed.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted</p>
<p><b><i>Control Objective:</i></b>  <b>SD-2: Controls provide reasonable assurance that access controls to enforce segregation of duties are established.</b></p>		
<p><b>Management reviews effectiveness of control techniques.</b></p> <p>Self-inspections of traditional security are conducted annually by SM.</p> <p>Self-assessments of systems access are conducted periodically at direction of IAM.</p>	<p>Inquired of management on whether reviews were performed to assess the adequacy of segregated duties.</p>	<p>Two out of six sites did not have comprehensive procedures that required performance reviews to assess the adequacy of segregated duties.</p>

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p><b>Control Objective:</b>  <b>SD-3: Controls provide reasonable assurance that personnel activities are controlled through formal operating procedures and supervision and review.</b></p>		
<p><b>Formal procedures guide personnel in performing their duties.</b></p> <p>Local and enterprise standard operating procedures identify tasks and functions required to enable personnel to perform their duties.</p>	<p>Inquired of supervisors and operations personnel to determine if standard operating procedures existed.</p> <p>Inspected standard operating procedures that guide personnel in performing their duties and determined whether they:</p> <ul style="list-style-type: none"> <li>• outline the proper steps for performing key functions, and</li> <li>• reflect the current operating environment.</li> </ul>	<p>No relevant exceptions noted.</p> <p>Three out of six sites did not have local standard operating procedures to guide personnel in performing their duties; however, personnel were supervised and enterprise policies and procedures were in place.</p>
<p><b>Active supervision and review are provided for all personnel.</b></p> <p>Operational activities are monitored by supervisors in accordance with procedures stated in the CS Security Handbook.</p>	<p>Inquired of supervisors and personnel to determine the process for monitoring operational activities.</p> <p>Inquired of site management to determine whether operations were being monitored by supervisors as stated in the CS Security Handbook.</p>	<p>No relevant exceptions noted.</p> <p>No relevant exceptions noted.</p>

## Service Continuity

Control Techniques (Related Controls Placed in Operation)	Test of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p><b>Control Objective:</b>  <b>SC-2: Controls provide reasonable assurance that data and program backup procedures and environmental controls have been implemented.</b></p>		
<p><b>Data and program backup procedures and environmental controls have been implemented.</b></p> <p>Full-volume weekly backups are covered as basic services.</p> <p>All backup data files are stored off-site. There are normally three different backup cycles (grandfather, father, son) held at the off-site location. The backup sites are required to be, at a minimum, 25 miles from the supported computing site.</p> <p>Each site has implemented its own off-site and transportation agreements. Most sites use some type of locked containers, and inventory system of containers are either provided by the contracting service or locally purchased.</p>	<p>Inspected policies and procedures for backing up data files for applications and networks.</p> <p>Inspected to determine whether procedures were in place to assure the physical and logical protection of the backup hardware.</p> <p>Inspected to determine whether sites had procedures that identified an off-site location for storage of backup tapes.</p> <p>Inspected to determine how often the site:</p> <ul style="list-style-type: none"> <li>• created backups,</li> <li>• rotated backups off-site,</li> <li>• tested the backups for completeness of data,</li> <li>• tested the backups for potential usability, and</li> <li>• retained the backup media.</li> </ul>	<p>Six out of sixteen sites did not have formal documented tape backup procedures that were consistently followed.</p> <p>No relevant exceptions noted.</p> <p>Two out of sixteen sites did not have procedures that identified an off-site location for storage of backup tapes.</p> <p>Thirteen out of sixteen sites did not have procedures to recover corrupted data files, lost programs, and operating systems by periodically testing backup tapes.</p>



<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
<p>Environmental Controls comprise the following controls.</p> <ul style="list-style-type: none"> <li>• Computing facilities and support areas have automatic notification of activation of smoke detectors that alarm locally and at supporting fire department.</li> <li>• Some administration areas have</li> </ul>	<p>Inspected a listing of personnel authorized to access off-site facilities to determine if access was appropriate based on job function.</p> <p>Inspected a listing of tape backups stored off-site to determine that:</p> <ul style="list-style-type: none"> <li>• tape backups existed,</li> <li>• files could be used to recreate current reports, and</li> <li>• tape backups were transported to the off-site facility and back to original location.</li> </ul> <p>Inspected to determine whether the off-site location:</p> <ul style="list-style-type: none"> <li>• was geographically removed from the primary site,</li> <li>• had adequate physical and access controls,</li> <li>• had boundary defense equivalent to the perimeter security at the primary site, and</li> <li>• had appropriate space for storage media and recovery documentation.</li> </ul> <p>Inspected data center and off-site facility to determine whether the following environmental controls were in place:</p> <ul style="list-style-type: none"> <li>• fire suppression and prevention mechanisms that automatically activate when they detect heat, smoke, or particles;</li> <li>• smoke detectors;</li> <li>• fire extinguishers and sprinklers;</li> </ul>	<p>Three out of sixteen sites did not fully implement procedures to restrict access to off-site facilities.</p> <p>Ten out of sixteen sites did not fully implement procedures to recover backup tapes stored offsite.</p> <p>Ten out of sixteen sites did not fully implement procedures to control access to these sites or facilitate recovery of operations.</p> <p>Nine out of sixteen sites did not fully implement environmental controls.</p>

<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
<p>automatic notification of activation of smoke detectors. Some of these only alarms locally; some alarm locally and at the supporting fire department.</p> <ul style="list-style-type: none"> <li>• Fire inspections are made based on local site rules.</li> <li>• Computing facilities and support areas have automatic activation of fire suppression systems.</li> <li>• Administration areas have either automatic activation of fire suppression systems or hand-held extinguishers located throughout the area.</li> </ul> <p>All computer facilities have:</p> <ul style="list-style-type: none"> <li>• automatic humidity and temperature controls systems that alarm when established humidity and temperature conditions are exceeded;</li> <li>• a master power switch located at or near the main entrance, which is labeled and protected by a cover to prevent accidental shut-off;</li> <li>• automatic voltage control systems that alarm if the voltage fluctuates beyond established safe operations levels;</li> <li>• a minimum of two electrical feeds;</li> <li>• battery powered uninterrupted power system to provide sufficient</li> </ul>	<ul style="list-style-type: none"> <li>• water detectors;</li> <li>• air conditioning systems;</li> <li>• humidity control systems;</li> <li>• uninterrupted power supply;</li> <li>• backup generators;</li> <li>• emergency lighting;</li> <li>• automated voltage control; and</li> <li>• redundant systems.</li> </ul> <p>Inspected to determine whether the data and network center staff were aware of the locations of:</p> <ul style="list-style-type: none"> <li>• fire alarms,</li> <li>• fire extinguishers, and</li> <li>• master power switches and emergency cut-off switches.</li> </ul>	<p>No relevant exceptions.</p>

<b>Control Techniques (Related Controls Placed in Operation)</b>	<b>Test of Operating Effectiveness</b>	<b>Results of Tests of Operating Effectiveness</b>
<p>power to all systems in the computer room to allow for at least 20 minutes of operations; and</p> <ul style="list-style-type: none"> <li>• backup generators that are set to automatically start-up and generate power when commercial power fails. The generators are tested monthly for operations and power generations. Additional fuel and spare parts are on hand to provide for sustained operations.</li> </ul>		

---

## **Section IV: Supplemental Information Provided by DISA**

---



## **Introduction**

This Statement on Auditing Standards No. 70 (SAS 70) audit resulted in the identification of potential vulnerabilities and process improvement within the areas of Information Security. The audit of DISA CS and associated FSO support, was designed, conducted, and reported, in accordance with standards of the American Institute of Certified Public Accountants and generally accepted government auditing standards. CS focuses its information system security around and in accordance with DoD Information Technology Security Certification and Accreditation (DoD Instruction 5200.40) and other directives.

Connecting a computer to a network inherently introduces security risk to both the computer and the network. The DITSCAP clearly places the responsibility of balancing IT system availability, interoperability, and security on the DAA. The DAA is responsible for the agency's systems certification and accreditations and the operating sites' authority to operate. The DISA DAA and FSO have provided CS with objective and measurable system security requirements that balance levels of risk with military operational need for availability and interoperability. Those criteria are delineated strategically and operationally via security instructions and guides, and tactically via measurable systems configuration criteria. FISCAM was the basis for the SAS 70 objectives and techniques. FISCAM is a standard methodology used in the Federal government. Accordingly, management clarified the techniques throughout the engagement to reflect the CS control environment. Throughout this engagement, CS management continued to clarify DoD techniques that deviated from the FISCAM methodology.

The results of the SAS 70 audit do provide some actionable and valuable strategic focus that will aid CS in solidifying security processes and in guiding overall migration toward a centrally managed enterprise following its recent Transformation (described below). Based upon lessons learned from this initial SAS 70 audit process, it is expected that future audits will enable an assessment of security posture that will result in less reportable vulnerabilities.

## **DISA's Computing Transformation**

The Combat Support Computing mission is to provide secure, interoperable, and assured data processing that enables the DoD to deploy, employ, and sustain a warfighting force. Just as the private sector maximizes advances in technology to improve service delivery and harvest savings, CS continues to take advantage of transformational technologies in order to improve enterprise IT infrastructure and provide the warfighter with "best value" computing support. Transformation strategies and objectives for CS include the following:

- refine processing, support, and services architecture while taking advantage of increased bandwidth and highly distributed computing and storage capability;
- provide standardized, content-rich computing environments;
- increase system availability by expanding data replication and mirroring;

- increase use of centralized automated systems management;
- continue workload consolidation where economies of scale can be achieved;
- facilitate transfer of additional processing support for command and control and intelligence functions into DISA facilities; and
- continue ongoing efforts to support cross-component server applications and facilitate DoD-wide consolidation as the designated provider for all DoD server processing.

Over the past 30 months and throughout the course of the SAS 70 audit, CS was engaged in executing a large-scale consolidation plan that included numerous workload migrations, introduction of new technologies, a comprehensive business and operational management restructuring, and a reduction-in-force that impacted over 1,000 government positions. This highly successful transformation is nearing completion and has included operational and technical transitions encompassing 28 mainframe logical partitions, over 800 customer applications, and over 850 geographically disparate network devices. A review of this report, or any evaluation of security processes, procedures, and management controls for CS (or their FSO support), must necessarily consider the impact of these transformational changes and the day-to-day operational imperatives that remained in effect during the period of this audit. Accordingly, the following is provided as a summary of CS's computing transformation.

### **Transformation Highlights**

The 2003-2005 transformation of CS represented yet another major step forward in providing cost effective combat support computing to the warfighters. Most importantly, the transformation will allow DoD to preserve military control over combat support processing as an integral component of the GIG and the "best value" option. The following summarizes the key elements of this transformation:

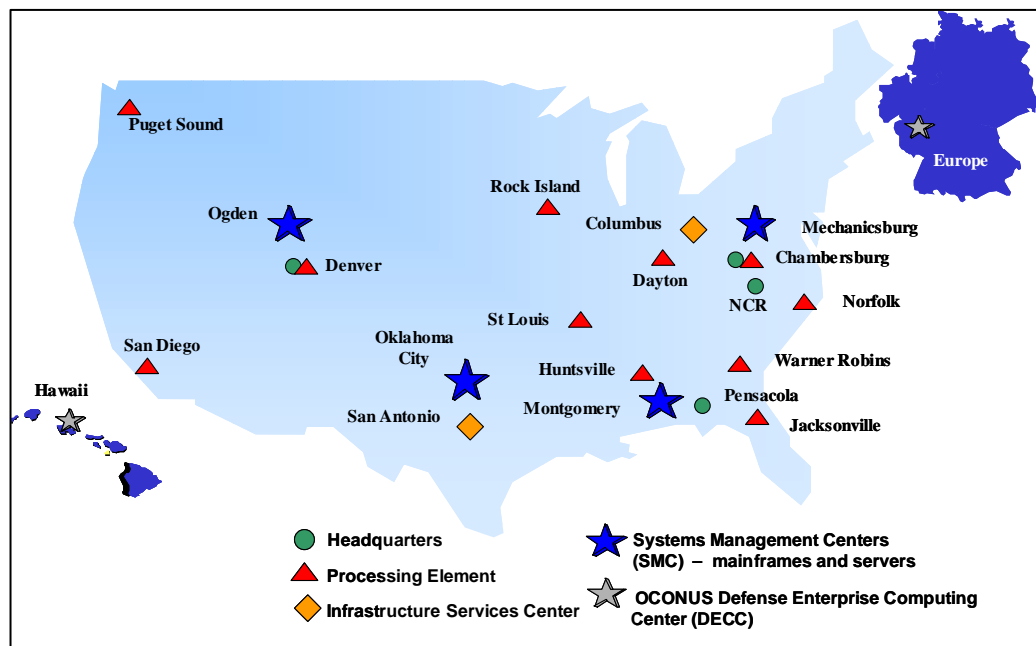
1. Implementation of assured computing. CS has fully implemented IBM mainframe assured computing that includes a set of initiatives designed to enhance facilities, equipment, communications, and software to ensure that data is continuously available to the warfighters. This has transformed traditional disaster recovery and continuity of operations planning processes to yield previously unattainable levels of availability. Foremost among these initiatives are measures to use remote data replication and mirroring at geographically separate locations to protect against the catastrophic loss of a processing facility, and to mitigate the risks inherent in data center consolidations. CS had previously proven this capability in the Unisys mainframe environment.
2. Consolidation of mainframe processing. CS operated six mainframe processing sites, five of which supported OS/390 and Z/OS (IBM-based) processing and three of which supported Unisys processing. Mainframe workload was consolidated into three IBM and two Unisys sites in conjunction with implementation of data mirroring and replication.
3. Consolidation of server processing. CS supported UNIX and Windows NT-based server processing at 15 locations. From FY 2003 to FY 2005, management and administration of these servers were consolidated into four sites, grouped primarily according to the supported Service or Defense agency customer. Given

the scope and distribution of Defense Finance and Accounting Service systems, a significant portion of the server consolidation involved Defense Finance and

Accounting Service applications. Some consolidations entailed physical relocation of assets, most; however, were logical migrations of the management functions.

4. Consolidation of systems management. CS consolidated all systems management functions for mainframe and server computing into four locations with primary and backup support for each operating environment. A “lights-dim” approach, with touch labor support for remote operations, was implemented at operating sites. Systems management consolidation was implemented in concert with mainframe and server processing consolidation from FY 2003 to FY 2005.
5. Management restructuring. To achieve further economies of scale in the management and administration of computing operations, CS centralized all business and operational support functions. Over the past 30 months, the former DECC and Detachment structures were eliminated. By the end of FY 2005, CS will consist of one Headquarters component, four production sites (or SMCs), two infrastructure services sites, and several “lights-dim” server processing sites, as described above. All business, financial, engineering, acquisition, logistics, and administrative functions currently performed in the field today are being integrated and consolidated into a single virtual management organization. The post-transformation site configuration is displayed in Figure 1.

**Figure 1. DISA Computing Services Site Configuration**



### Technology Insertion and Technical Management Changes

In recent years, significant advances have been made in the areas of IT enterprise architectures and management automation. Networks have been designed to separate



management functions from in-band production, thereby increasing security and enabling remote administration of devices and applications. Toolsets have been developed that provide administrators with increased capacity to manage customers' systems, resulting in far superior ratios in terms of environments managed per operator. During the planning phase for the current transformation, CS performed extensive industry research and incorporated these concepts into its transformation design. The following briefly summarizes some of the capabilities implemented to support the FY 2003-2005 transformation that were still being fully established during the course of the subject SAS 70 audit.

### ***Central Communication Centers***

CS established two CCCs to provide centralized network management for all 18 DECC sites, thereby improving standardization and configuration management while achieving significant economies of scale. The core CCC function is to maintain a secure, cost effective, efficient, and reliable telecommunications operations environment supporting DoD and the warfighters by providing the appropriate event correlation for network and security environments within the data centers, and to serve as the SMC escalation organization to the Defense Information System Network Regional Network Operations Center, the Service, and Defense agency base level management centers. Utilizing a secure "out-of-band" management network, the CCCs support all routing, switching, Domain Name Servers, wide area network connectivity to DISA Network Services, and network security device operations. The CCCs also employ a Security Management Team that maintains the security functions on the production networks managed by the CCCs, including access control and IDS, firewall operations, and configuration management.

### ***Out-of-Band (OOB) Network***

The CS out-of-band management network was designed and implemented to support secured remote administration of all CS "glass house" (i.e., inside the data center) devices. The out-of-band infrastructure is designed to provide a secure method for remote privileged user access and Enterprise System Management data transmission, irrespective of whether SMC personnel are physically located in the same building. The out-of-band architecture includes virtual private network connectivity and privileged user access accounts based upon the specific functions required by the user. Separate individual user access profiles are issued for Windows, UNIX, and mainframe environments, and network access and authentication is validated for auditability. Internet Protocol Security tunnels are established among all DECCs to the Enterprise System Management suites located at the two CCC locations for encrypted system management data. Tivoli and Hewlett Packard Openview collectors that reside within the out-of-band collect site-specific management data that is then transferred to the central complex in Oklahoma City and Montgomery.

### ***Remote Systems Management***

One of the key elements of the CS Transformation was to establish remote system administration capabilities. Previously, all 16 data centers maintained operational control independently, which resulted in use of multiple toolsets and procedures. To improve standardization and reduce the ratio of system support personnel to the number of devices managed, CS made remote systems management a priority and shifted the paradigm from local ownership and control to that of a virtual enterprise environment. Enterprise System Management software, such as Hewlett Packard Openview, Tivoli TEC (Tivoli Enterprise Console), and Veritas Back-up, was integrated into a common architecture for

use by all SMCs. In addition, with remote management as CS's premise, a complete review of systems administration from an enterprise perspective was performed and resulted in more efficient and standard ratios for all mainframe, windows, and UNIX environments. As discussed above, an out-of-band network infrastructure was designed and implemented as the vehicle to provide secure access for remote system management personnel.

### ***Central Staging Center***

To ensure proper configuration management within the transformed CS, the Operations Division established a "Central Staging Center" to serve as a centralized receipt and staging function for all server and communications hardware and software destined for implementation at DECC locations. This capability represented a marked improvement in configuration control by ensuring that all assets received are documented in a standard fashion with the standard asset management tools, and staged in accordance with the prescribed configuration process. Centralization ensures that all standard process requirements and coordination associated with the incorporation of new assets into the production operating environment are consistently met, and simplifies large-scale implementations involving assets in multiple locations. Responsibilities include mid-tier and communications configuration setup, and application of STIG implementation at the operating system, database, network, and web levels. This CS component is staffed with logistics and technical personnel to provide asset management and inventory support and ensure that all configuration management databases are reconciled.

## **Security Processes and Other Considerations**

### **Management Restructuring and Transitions**

As part of the Transformation plan to centralize all business and operational support functions within CS, management of all security aspects (information, physical, personnel, etc.) was foremost in terms of departing from the previous decentralized management structure inherent in the 5 DECC and 13 Detachment configuration. Centralized control, development, and review of all PEs' SSAAs and authority to operate documents were implemented site-by-site. Documents and processes were in the process of migration from field to centralized management, including transfer of documents and training of new personnel, throughout the period of the SAS 70 audit process.

Other functions and processes supporting field unit security were also in a state of transition during the SAS 70 audit. For example, configuration management responsibilities, initially planned for centralization, were largely redistributed to the field units, and staff positions were re-instated pending the acquisition of an automated tool. Technical challenges and delays in fully implementing Enterprise System Management tools that support the centralized assessment of security status (such as the self-healing SRRs and the 6.0 release of FSO's VMS) have impacted plans to centralize, which has required re-instatement of field-level security monitoring and processes beyond the planned dates. The out-of-band for SIPRNet and NIPRNet, the installation of separate administrative and production local area networks at all sites, and the migration of all non-production workload to the production local area networks took place during the SAS 70 audit. In addition, while this was taking place, the entire CS network infrastructure was migrating toward a new, closed architecture.

During this dynamic transition, CS continued to make significant improvements in its security posture. Examples include the implementation of deny-by-default networks, automated SRRs, closing of ports at the internet-NIPRNet gateways, implementation of network security components, daily tracking of Information Assurance Vulnerability Alert compliance, an auditable network change process, an auditable connection-approval process, encryption of many file transfers and interactive sessions, implementation of Microsoft patch servers, and etc.

### **Security Updates and Coordination**

Installations of Information Assurance Vulnerability Alerts, software patches, and customer application releases are major causes for scheduled outages. Since CS must balance customer operational imperatives with Information Assurance Vulnerability Alert and STIG compliance, customer coordination must be obtained early, followed by rigorous adherence to established timeframes, so that vulnerabilities can be eliminated. During the SAS 70 audit, situations requiring this customer coordination took place; however, customer approval for the downtime required to implement security improvements was not always attainable.

### **Improved Security Processes**

During the SAS 70 audit, many of the findings at various sites were corrected on the spot and improved processes were established. While insights gained from external examiners were helpful, the final report covers the entire set of objectives for CS as a whole and, accordingly, does not reflect all iterative corrections and enhancements made at individual sites. The following are examples of some of the improvements:

- Several updates to the System Security Authorization Agreement were made during the audit. Additional security policies and procedures were incorporated into the System Security Authorization Agreement that conformed to the recommendations.
- The process for managing DD Form 2875s was modified to ensure they are filled out in a consistent manner and proper authorization for system access is maintained.
- The Security Awareness training program was strengthened at the Headquarters level to ensure that all employees are completing the training on an annual basis.
- Out-processing procedures were refined to ensure all employees (contractor and government) follow the same procedures when their employment terminates.
- Tiger Teams were established to develop or refine procedures in areas where the SAS 70 auditor recommended improvements.

## **Continuity of Operations Plan**

CS has an up-to-date contingency plan developed and documented. The Business Continuity Plan (BCP) is a contingency plan that, by regulatory requirements within and external to CS, each CS processing site must develop, maintain, and exercise. CS must keep the BCP up to date, and have the plans evaluated annually for completeness and

accuracy. Based on exercise results, the plan is updated to address identified discrepancies. The BCP is reviewed annually and tested periodically.

Each CS-managed application has a recovery strategy documented that identifies the process for recovering that application in response to a disaster or contingency related event. All BCP information, including information on alternate recovery sites and telecommunications, is reviewed annually for accuracy and completeness. During application recovery exercises, the capabilities of alternate sites and telecommunication facilities are confirmed. Where shortfalls exist, they are documented and addressed within the BCP and their capabilities are tested during subsequent exercises. As part of that documentation and where appropriate, alternate processing sites and telecommunication facilities are identified.

The BCP is reviewed annually for accuracy and completeness and subjected to a BCP walk-through exercise, using the appropriate team members, as well as an audit of the related off-site storage programs and facility. In addition, selected applications are subjected to application recovery exercises involving a physical relocation of primary production processing to a documented alternate location.

CS has established policies governing the timely development and distribution of exercise after action reports, as well as requirements for addressing identified discrepancies within the BCP. Action reports are due, in final form, within four weeks after the completion of any application recovery exercise. They are distributed to the appropriate customer personnel and are used as starting points for the updating and refinement of the relevant sections of the BCP.

## **Summary**

From the DISA perspective, this initial SAS 70 audit proved to be a challenging undertaking in terms of timing, process, and methodology. Performing an audit of this magnitude and complexity is undoubtedly a difficult task even in the most stable of operating environments. Attempting this in the middle of a full-scale transformation of the CS enterprise required unprecedented effort on everyone's part and, unfortunately, complicated the task for all involved. Notwithstanding limitations in the results obtained as discussed above, this audit has provided a foundation upon which to continue improving processes and procedures essential to maintaining proper information security in all areas.

# Acronyms and Abbreviations

BCP	Business Continuity Plan
CCC	Communications Control Center
CIO	Chief Information Officer
CS	Center for Computing Services
DAA	Designated Approving Authority
DECC	Defense Enterprise Computing Centers
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
IDS	Intrusion Detection System
ISC	Infrastructure Services Center
IT	Information Technology
MAC	Mission Assurance Category
OMB	Office of Management and Budget
OST	Operations Support Team
PE	Processing Element
SA	System Administrator
SAS	Statement on Auditing Standards
SM	Security Manager
SMC	System Management Center
SRR	Security Readiness Review
SSO	Systems 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**

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 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

## **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

## **Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (cont'd)**

House Subcommittee on Defense, Committee on Appropriations

House Committee on Armed Services

House Committee on Government Reform

House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform

House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform

House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

## Team Members

The Defense Financial Auditing Service, in conjunction with contract auditors from Price Waterhouse Coopers and the Technical Assessment Division of the Department of Defense Office of the Inspector General (DoD OIG), prepared this report. Personnel of the Quantitative Methods Division, DoD OIG, also contributed to the report.

Paul J. Granetto  
Patricia A. Marsh  
Addie M. Beima  
Michael Perkins  
Kenneth H. Stavenjord  
Suzette L. Luecke  
LTC Shurman Vines  
Peter C. Johnson  
Ahn Tran  
Michael Davitt  
Chanda D. Lee  
Jason E. Alt  
Walter J. Carney  
Eric T. Thacker  
Cindy L. Gladden  
Chi H. Lam  
Brian M. Stumpo  
Wen-Tswan Chen