May 18, 2006

Information Technology Management

Report on General and Applications Controls at the Defense Information Systems Agency, Center for Computing Services

(D-2006-086)

~~**SPECIAL WARNING**~~

~~This report contains information exempt from mandatory disclosure under the Freedom of Information Act, Exemption 2~~.

Department of Defense
Office of Inspector General

Quality *Integrity* *Accountability*

Additional Copies

To request additional copies of this report, contact Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact 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

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

May 18, 2006

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on General and Application Controls at the Defense Information Systems Agency, Center for Computing Services (Report No. D-2006-086)

We are providing this report for information and use. We considered management comments on a draft of this report when preparing the final report.

Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the staff. Questions should be directed to (b) (6) [redacted]. For the report distribution, see Appendix E. The team members are listed on the inside of 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

Department of Defense Office of Inspector General

Report No. D-2006-086 **May 18, 2006**
(Project No. D-2004-D000FG-0191.001)

General and Application Controls at the Defense Information Systems Agency, Center for Computing Services

Executive Summary

Who Should Read This Report and Why? Department of Defense personnel who manage the services provided by Defense Information Systems Agency, Center for Computing Services (CS) may find this report of interest, as will other CS user organizations and their independent auditors. Persons who supervise any part of the Department of Defense Information Assurance program may also find this report useful. This is one of three reports in support of the overall Statement on Auditing Standards No. 70 audit. This report describes compliance with certain general and application control objectives, as well as compliance with applicable laws and regulations, including the Department of Defense Information Technology Security Certification and Accreditation Process. The other reports describe the results of testing of configuration settings on selected assets in the CS environment and the results of penetration testing at selected CS sites. These reports collectively identify weaknesses related to general and applications controls, recommend corrective actions, and identify where CS has already taken action.

Background. The DoD Office of Inspector General is implementing a long-range strategy to conduct audits of DoD financial statements to comply with the Chief Financial Officers Act of 1990 (P.L. 101-576), as amended, which requires agencies to prepare and submit to Congress audited financial statements. As part of this effort, we performed a Statement on Auditing Standards No. 70 audit of CS in accordance with Generally Accepted Government Auditing Standards and American Institute of Certified Public Accountants standards. CS provides computer processing for the entire range of combat support functions, including transportation, logistics, maintenance, munitions, engineering, acquisition, finance, medicine and military personnel readiness. With more than 800,000 users, CS provides support for over 1,400 applications in 18 geographically separate facilities utilizing more than 40 mainframes and 3,000 servers. The reliability of general computer controls directly impacts individual financial and accounting systems and feeder systems, and, ultimately, could impact the ability of DoD to produce reliable and auditable financial statements.

Results. Controls associated with the CS entity-wide security program, system access, computer program changes, systems software, segregation of duties, and service continuity needed improvement to ensure that CS information systems operated effectively and provided appropriate confidentiality, integrity, and availability. Without standardization in policies and procedures throughout the CS environment, controls may not be consistently implemented to meet DoD security requirements; consequently, impacting security across the CS environment. Specifically:

- CS had not developed and implemented an effective entity-wide information security program across the Defense Enterprise Computing Centers. CS needs to implement risk assessments, security plans, current and standard security policies and procedures, a central security management structure, and communicate individual security responsibilities. See finding A of the report for detailed recommendations.

- General controls over account management were not adequately designed and not operating effectively to ensure that only authorized users had access to systems and that user accounts were being removed in a timely manner. CS needs to establish standard account management procedures to provide proper controls over user access. See finding B of the report for detailed recommendations.

- CS had not implemented effective procedures for monitoring and maintaining audit trails. CS needs to implement consistent procedures over the creation, review, and maintenance of audit trails. See finding C of the report for detailed recommendations.

- CS did not have effective controls over developing, maintaining, and testing contingency plans, and the controls did not fully comply with Federal and DoD requirements. CS needs to establish an entity-wide continuity of operations plan, supplemented by site-specific plans, and standard policies and procedures over testing to ensure current and comprehensive continuity of operations plans. See finding D of the report for detailed recommendations.

- CS had not developed adequate procedures to effectively manage data backups and the off-site storage facilities did not have adequate physical and environmental controls. CS needs to develop and implement standard data backup policies and procedures to ensure timely recovery of all production systems and data. See finding E of the report for detailed recommendations.

- CS had not implemented sufficient physical and environmental controls to adequately safeguard equipment and to fully comply with DoD policy. CS needs to implement procedures to ensure that the computing facility have sufficient physical and environmental controls. See finding F of the report for detailed recommendations.

- CS management had not implemented standard and effective change management policies and procedures across sites. CS needs to develop and implement standard policies and procedures over the change management process to ensure proper modification to the computing environment. See finding G of the report for detailed recommendations.

- CS had not implemented effective application controls over system access and security monitoring of the Enterprise Systems Management applications to ensure that only authorized users had access to these systems. CS needs to develop and implement comprehensive application controls to prevent unauthorized access, unauthorized disclosure of critical information, and loss of resources. See finding H of the report for detailed recommendations.

Management Comments and Audit Response. The Director, Center for Computing Services concurred with all 46 recommendations directed to CS and the Chief, Field Security Operations (FSO) concurred with the 3 recommendations that were redirected to the FSO. See the individual findings for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.

Table of Contents

Findings

Appendixes

Management Comments

Background

The Defense Information Systems Agency (DISA), Center for Computing Services (CS), provides computer processing for a wide range of combat support functions, including transportation, logistics, maintenance, munitions, engineering, acquisition, finance, medicine, and military personnel readiness. With more than 800,000 users, CS processes over 1,400 applications in 18 geographically separate facilities utilizing more than 40 mainframes and 3,000 servers. In March 2003, CS officially announced its plans for transformation for its continental United States (CONUS) facilities. The CS transformation consists of four initiatives: (1) mainframe consolidation, (2) systems management center consolidation, (3) Defense Finance and Accounting Service server consolidation, and (4) management restructuring. CS sites outside of CONUS were not included in the transformation. Transformation would result in CS being highly centralized, highly standardized, secure, and efficient. See Appendix C for additional information on the transformation.

CS processing facilities encompass sixteen locations across the CONUS, as well as two overseas locations. CS has adopted a strategy for assured computing by implementing initiatives to ensure information and mission critical applications are continuously available to its customers. These initiatives include facilities upgrades, improved equipment availability, diverse and redundant communications, improved software availability, and measures to remotely replicate data. Assured computing, coupled with the ability to rapidly increase processing and storage capacity via utility contracts, enables CS to meet customer requirements for availability and surge capabilities. CS offers computer processing services for DISA-owned and customer-owned platforms. Services include computer operations, data storage, systems administration, security management, capacity management, systems engineering, web and portal hosting, architectural development, and performance monitoring.

At the CS Headquarters level, the Chief of Operations reports directly to the CS Director. The Chief of Operations has the overall responsibility for issuing operations standards, policies, plans, standard business processes, and standard operating procedures. Subordinate to CS Headquarters are the operating sites, designated as Defense Enterprise Computing Centers (DECCs). DECC responsibilities include production operations, such as site operating functions that directly support customer requirements, as well as technical and customer support functions. The DECCs in the CONUS were divided into the following four functional designations.

- **System Management Centers.** The primary responsibility of each System Management Centers (SMCs) is systems management and customer support functions for the mainframe and server computing environments. The SMCs are located in Mechanicsburg, Pennsylvania; Montgomery, Alabama; Ogden, Utah; and Oklahoma City, Oklahoma.

- **Infrastructure Services Centers.** The Infrastructure Services Centers (ISCs) perform system management for specialized fielding efforts from

CS customers. The ISCs are located in Columbus, Ohio; San Antonio, Texas; and St. Louis, Missouri.

- **Processing Elements.** Facility management, hardware support, physical security, touch labor[1] for communication devices, and touch labor for media management are the primary responsibilities of a Processing Element (PE). The PEs are located in Chambersburg, Pennsylvania; Dayton, Ohio; Denver, Colorado; Huntsville, Alabama; Jacksonville, Florida; Norfolk, Virginia; Rock Island, Illinois; San Diego, California; and Warner Robins, Georgia.

In addition to the DECCs, CS established two Communications Control Centers (CCCs) to provide centralized network management for all DECCs to maintain a secure, cost effective, efficient, and reliable telecommunications operations environment. The CCCs support all routing, switching, domain name servers, wide area network connectivity to DISA Network Services, and network security device operations. The CCCs are located at DECCs Montgomery and Oklahoma City.

The Field Security Operations (FSO) is an organization within DISA that conducts vulnerability scans and annual reviews of CS for compliance with Security Technical Implementation Guides (STIGs).

DoD Information Assurance Requirements. DoD Directive 8500.1, “Information Assurance,” October 24, 2002, and DoD Instruction 8500.2, “Information Assurance Implementation,” February 6, 2003, provide the baseline for the DoD Information Assurance (IA) Program and lays out five essential competencies to ensure a successful risk management program. The five essential competencies are the ability to:

- assess security needs and capabilities,
- develop a purposeful security design or configuration that adheres to a common architecture and maximizes the use of common services,
- implement required controls or safeguards,
- test and verify, and
- manage changes to an established baseline in a secure manner.

The DoD Instruction 8500.2 defines mission assurance category (MAC) and confidentiality levels. The MAC level 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. The confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access a system, including intranet, Internet, and wireless access. The STIGs are written to MAC II sensitive, which are systems handling

[1] Touch labor is the physical on-site work needed, when the systems are being remotely managed.

information that is important to the support of deployed and contingency forces and the loss, misuse, or unauthorized access to or modification of the information could adversely affect the national interest or the conduct of Federal programs, or an individual's privacy.

DoD Instruction 5200.40, "Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, establishes a standard department-wide process, set of activities, general tasks, and management structure to certify and accredit information systems and maintain the IA and security posture of the defense information infrastructure throughout the life cycle of each system. The certification process is a comprehensive evaluation of the technical and non-technical security features of an information system or site. The process establishes the extent to which a particular design and implementation meets specified requirements for physical, personnel, administrative, information, information systems, and communications security. The accreditation process is a formal declaration by the Designated Approving Authority that an information system or site is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

General Controls. General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help to ensure proper operation. Some primary objectives for general controls include safeguarding data, protecting computer application programs, precluding unauthorized access to system software, and helping to ensure continued computer operation in case of unexpected interruptions. The Government Accountability Office (GAO) Federal Information System Controls Audit Manual (FISCAM) describes six major categories of general controls. These six categories are:

- entity-wide security program planning and management,
- access controls,
- application software development and change control,
- system software,
- segregation of duties, and
- service continuity.

Application Controls. Application controls are directly related to individual computerized applications owned and operated by CS to manage, operate, and secure the computing environment. These controls help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. Application controls include application access controls, such as technical security features and security configuration settings; programmed control techniques, such as automated edits; and manual follow-up of computer-generated reports, such as reviews of reports identifying rejected or unusual items. General and application controls should be effectively designed and implemented to help ensure the reliability, appropriate confidentiality, and availability of critical automated information.

Objectives

The overall audit objective was to evaluate whether CS implemented controls to ensure that its systems and processes were secure and complied with significant applicable guidance and requirements. Specifically, the audit objective was to determine whether CS: (1) general and application controls were adequately designed and effectively operating; (2) complied with the Federal Financial Management Improvement Act and all other applicable laws and regulations; and (3) properly certified and accredited its computing environment in accordance with DITSCAP. This report contains the results from general and applications controls testing in support of the three objectives noted above. Two other technical reports, Diagnostic Testing at Defense Information Systems Agency, Center for Computing Services, and Penetration Testing at Defense Information Systems Agency, Center for Computing Services, provide additional support for these objectives. See Appendix A for a discussion of the scope and methodology of our review and prior audit coverage related to the objectives.

A. Security Program

A CS entity-wide information security program had not been fully developed and implemented consistently across all sites. CS lacked an entity-wide security program because:

- CS management had not implemented an entity-wide risk assessment program,
- CS did not have complete and current security plans,
- CS did not update policies to adequately reflect current Federal and DoD policies, and
- CS had not established an effective central security management structure and fully communicated individual security responsibilities.

Without an effective and standardized security program throughout the CS environment, the risk is increased that controls will not be consistently implemented to meet minimum system security requirements, which impacts the security of the entire CS environment.

Information Security

CS had not developed and implemented an effective and comprehensive entity-wide information security program. An entity-wide information security program is the foundation for the agency's security control structure and demonstrates management's commitment to mitigating security risks. The Federal Information Security Management Act (FISMA) provides guidance requiring the development, documentation, and implementation of an entity-wide information security program. An entity-wide program would provide information security for systems that support the operations and assets of the entity. FISMA requires that the agency-wide information security program include:

- periodic assessments of risk,
- subordinate security plans to provide adequate information security for facilities and systems or groups of information systems, and
- designation of security responsibilities through security awareness training.

DoD Instruction 8500.2 establishes security requirements which apply to the definition, configuration, operations, interconnection, and disposal of DoD information systems. The IA controls developed under this requirement form a management framework for the allocation, monitoring, and regulating of IA resources that is consistent with Federal guidance provided in Office of Management and Budget Circular No. A-130 (OMB A-130), "Security of Federal Automated Information Resources," November 28, 2000. OMB A-130 requires that agencies implement and maintain an information security program to assure that adequate security is provided for agency information that is collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

Prior to the transformation, each DECC maintained its own security program and systems. However, because of the transformation, many of the functions at each DECC including business management, resource management, engineering, acquisition, and logistics are being centrally managed. The transformation plan did not identify security as a function to centrally manage. With the transformation, the DECCs are becoming more interdependent of each other. Systems are being remotely managed and the networks are being standardized and centrally managed. A standardized and centrally managed security program implemented throughout the CS environment will reduce the risk of inconsistently applied controls and provide better assurance that the minimum system security requirements are met for the entire CS environment.

Risk Assessments

CS management had not implemented an entity-wide risk assessment program that was comprehensive and designed to address the range of risks that could expose CS to security vulnerabilities. The identification of these risks is needed to develop an effective entity-wide information security program. CS had not developed a risk assessment that was entity-wide; the risk assessments were developed for each site. CS used the DITSCAP process and Security Readiness Reviews, including network vulnerability studies, physical security reviews, and compliance audits, to analyze the risk to individual sites. The DISA transformation integrated and consolidated several of the business functions at the headquarters level and DECCs began remotely managing assets at other DECCs. To ensure that the risk assessments cover all necessary areas, an entity-wide risk assessment is needed. The entity-wide risk assessment should take into consideration the site specific risk assessments to provide the aggregate risk to the environment.

In addition to developing an entity-wide risk assessment, the DECCs need to follow a standard methodology in conducting individual site risk assessments. The FSO issued a Risk Analysis Guide in November 2003; however, not all sites followed the guide. DECC St. Louis had developed risk assessments that did not conform to the Guide. Without an entity-wide risk assessment and a consistent approach at the sites, CS cannot ensure that a comprehensive review and analysis of its risks had been performed to fully address security vulnerabilities and potential weaknesses across the entity.

Security Plans

While the individual sites had developed individual site security plans, these plans were not always current or complete. For example, DECC St. Louis did not have a current and approved plan, and the plan for DECC Oklahoma City was also

outdated. In addition, the DECCs did not update these plans to keep pace with evolving technologies and the consolidation and movement of CS assets.
OMB A-130 requires the development of security plans and outlines the requirements of the plan. DoD Instruction 8500.2 requires that a security plan be established that describes the technical, administrative, and procedural IA program and policies and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, and emergency response).

Once developed, security plans should be implemented and consistently monitored, reassessed, and updated based on changes in the risk assessment and environment to help ensure effective security procedures are maintained. Because of the dynamic nature of the CS environment and the constant changes in technology, CS management needs to periodically reassess the adequacy and currency of the plans. Without current and complete security plans, CS increases the risk of having inadequate security controls and noncompliance with Federal and DoD policies.

Security Policies

CS did not keep its security policy up to date with the current Federal and DoD requirements. In addition, CS security policy also did not address segregation of duties as required by DoD Instruction 8500.2.

The Handbook. The DISA CS Security Handbook, December 1, 2000, (the Handbook) had not been updated to reflect DoD requirements. DoD Instruction 8500.2 was issued in February 2003 and defines a baseline level of IA for all DoD information systems through the assignment of specific IA controls for each system based on the MAC and confidentiality level. The Handbook covers topics like information systems security, personnel security, and industrial security and the DECCs used the Handbook in implementing their security programs. Updating the Handbook to current Federal and DoD requirements reduces the risk that the DECCs would inconsistently interpret and implement Federal and DoD policies.

Segregation of Duties. CS had not established formal policies and procedures to help ensure segregation of duties for sensitive positions. DoD Instruction 8500.2 requires implementation of the principles of least privilege and segregation of duties. For example, sensitive roles such as System Administrators and security functions need to be clearly defined and separated in order to ensure authorized access and least privilege principles. CS management had not clearly defined sensitive functions, incompatible duties, and prohibited activity through the development of formal policies and procedures. For example, DECCs Mechanicsburg, Montgomery, and Oklahoma City did not have policies and procedures describing segregation of duties. At DECC Columbus, personnel did not always comply with applicable segregation of duties policies and compensating controls were not developed to mitigate the risk of limited staff resources. Position descriptions for civilian personnel at DECCs Mechanicsburg and Oklahoma City did not address prohibited activities that are incompatible with the employee responsibilities.

The absence of clearly defined segregation of duties increases the risk that individuals may be assigned incompatible functions, increasing the risk of unauthorized disclosure of sensitive information. CS had little assurance that the database or systems administrator did not have privileged accounts for systems in a business environment which would be considered incompatible duties. For example, normal business practice would preclude the same person from having accounts payable duties, as well as disbursing responsibilities since that individual may be able to cover-up fraudulent activities.

Security Management and Responsibilities

CS had not established an effective central security management structure to manage, monitor, and ensure an adequate security posture across the entity. In addition, CS needs to improve communication of individual security responsibilities through security awareness training.

Security Management Structure. CS had not established an effective central security management structure to ensure that policies and procedures were being consistently applied across CS. Prior to the transformation, each DECC had autonomy to manage and maintain its operating environment and systems. With the transformation, the DECCs are becoming more interdependent with each other and require consistent standards that address information technology (IT) security policies across CS. However, there was no effective central security management role at the CS level to monitor and enforce an effective overall security program.

DoD Instruction 8500.2 outlines IAM (IAM) responsibilities as the individual responsible for the IA program of a DoD information system or organization. The IAM tracks compliance with the IA controls and reports IA management review items, such as certification and accreditation status, compliance with personnel security requirements, and compliance with training. With the size and complexity of CS, this is a considerable task. CS did not allocate enough resources to effectively accomplish the IAM responsibilities across CS. Without dedicated individuals in CS to carry out the IA responsibilities, CS may not be able to fully enforce security policies and procedures. Insufficient monitoring of the entire security program could unknowingly expose CS systems to vulnerabilities.

CS User Security Awareness and Training. CS needs to improve communication of individual security responsibilities through security awareness training and ensure that all personnel receive and document the appropriate professional training required to perform their duties. DoD Instruction 8500.2 requires that all DoD employees and IT users maintain a degree of understanding of IA policies and doctrine commensurate with their responsibilities and that they shall receive both initial and periodic refresher IA training. CS personnel were not consistently informed of, or trained in, their security responsibilities. Specifically, the security awareness training was not consistently provided for new employees and contractors, and not all employees consistently received the annual security awareness refresher training at DECCs Ogden and St. Louis. Employee training and professional development activities were not documented at DECCs Columbus, Oklahoma City, and Ogden.

In addition, personnel at DECCs Mechanicsburg, Montgomery, Ogden, and St. Louis, were not familiar with their responsibility for intrusion detection and incident response. The lack of an effective process to provide, monitor, and document specialized training and security awareness training may lead to inappropriate system use and may unknowingly compromise systems.

Summary

The new CS organizational structure requires a standardized approach to define and implement policies and procedures as part of an entity-wide security program. The entity-wide information security program should include risk assessments, security plans, current and standard security policies and procedures, a central security management structure, and a security awareness training program. Without comprehensive risk assessments, CS cannot identify and address its potential security vulnerabilities and weaknesses. CS increases its risks of having inadequate security controls if it does not have current and complete security plans and policies and procedures. The lack of current and standardized policies and procedures may result in noncompliance with Federal and DoD requirements and that controls would not be consistently implemented. In addition, CS may not be able to fully enforce security policies and procedure without a central security management structure. Finally, CS personnel might not be aware of their security responsibilities or perform inappropriate system operations without a standard security awareness training program. Therefore, the lack of an entity-wide information security program may negatively impact the security of the entire CS environment.

In order for CS to have an effective entity-wide information security program, CS also needs to improve controls over system access (findings B and C), service continuity (findings D, E, and F), configuration management (finding G), and internal system applications (finding H).

Recommendations, Management Comments, and Audit Response

A. We recommend that the Director, Center for Computing Services:

1. Implement a comprehensive risk assessment program for the entire Center for Computing Services that includes:

a. Establishing an entity-wide risk assessment.

Management Comments. The Director, CS, concurred and stated CS has established a risk assessment plan for each SMC, ISC, and PE within the CS enterprise as of February 2006. The CS organizational structures' complexity requires an individual risk assessment for each site to achieve an entity-wide risk assessment program.

Audit Comments. While the intent of the recommendation was a comprehensive risk assessment that addressed the entire CS, CS believes that an overall risk assessment is not needed. Instead, CS has standardized the process and updated the individual DECC risk assessments as part of an overall risk assessment program. As CS continues with their transformation into their target environment, we will continue to evaluate the need for an overall risk assessment and revaluate this recommendation in future audits. CS proposed actions is an acceptable solution for the current audit recommendation.

b. Applying site risk assessments consistently.

Management Comments. The Director, CS, concurred and stated the CS IAM developed a standard risk assessment template which has been implemented at all the PEs and will be used by the SMC and ISC IAMs when performing the annual update of risk assessment. This template went into effect in August 2005.

2. Implement a process to monitor the Defense Enterprise Computing Centers security plans to ensure that current Federal and DoD policies are adhered to, plans are current and approved, and address the results of the risk assessments.

Management Comments. The Director, CS, concurred and stated the CS IAMs have reviewed and updated all site annual security plans to address the risk assessment results. In addition, the plans have been approved.

3. Update Defense Information Systems Agency, Center for Computing Services Security Handbook to reflect current Federal and DoD policies.

Management Comments. The Director, CS, concurred and stated CS released a draft of an updated Security Handbook in February 2006. The Handbook draft version has been signed into effect, as policy, by a memorandum signed by the Deputy Director, CS on February 27, 2006. CS expects to release the final version of the Security Handbook in July 2006.

4. Develop and implement appropriate segregation of duties policies and procedures, which include documenting sensitive positions and incompatible and prohibited activities.

Management Comments. The Director, CS, concurred and stated CS created a segregation of duties policy and procedure. This policy went into effect March 15, 2006.

5. Establish a central security management structure to manage and monitor compliance with applicable Federal, DoD, and Defense Information Systems Agency policies.

Management Comments. The Director, CS, concurred and stated CS implemented an entity-wide Security Concept of Operations document effective February 2006.

6. Develop and conduct a standard security awareness training program which includes training for new employees and contractors and annual security awareness training.

Management Comments. The Director, CS, concurred and stated CS has mandated that all CS personnel take initial security awareness training before gaining access to the system and are required to take annual security awareness training. Training is recorded and maintained by the CS IAM and Security Manager. For CS Headquarters personnel within the National Capital Region, training is managed by the Manpower, Personnel, and Security Office within DISA. This was effective as of September 2005.

B. System Access

General controls over account management were not adequately designed and not operating effectively to ensure that only authorized users had access to systems and that user accounts were being removed in a timely manner. CS had inadequate account management controls because DECCs did not comply with CS user access policy and the CS Security Handbook did not provide specific guidance on some key aspects of account management. As a result, CS sites implemented dissimilar security procedures, and inadequate controls over account management increase the risk of unauthorized access and expose sensitive data to the risk of improper modification or deletion.

User Access

The controls over user access, including creation, maintenance, and deletion of individual accounts, were not adequately designed or operating effectively throughout the CS environment. DoD Instruction 8500.2 requires that a comprehensive account management process be implemented to ensure that only authorized users have access to workstations, applications, and networks. In addition, individual accounts designated as inactive, suspended, or terminated should be promptly deactivated. DECCs did not fully comply with CS access policy, and CS policy needs improvement to ensure the implementation of a comprehensive account management process.

User Access Policy

The DECCs did not comply with CS user access policy. The system access request forms did not exist or were incomplete. The incomplete forms lacked appropriate authorizations, did not identify the system, or were not consistent with users' actual level of access. In addition, some terminated employees still had access to CS systems.

Systems Access Authorization Request Forms. The Handbook requires that all users complete an access request form (System Access Authorization Request (SAAR) Form (DD Form 2875) or former DISA Form 41) to gain access to CS systems. The Handbook requires that user access forms include, at a minimum:

- identification of the system, application, and data sets;
- verification of the requested privileges from the supervisor;
- verification of the user's clearance from the security manager;
- verification of a need-to-know from the data owner; and
- acknowledgement of the relevant security responsibility from the user.

In addition, the Handbook requires that CS maintain the access form for the life of the user account and one year after the account is deleted. We selected a judgmental sample of 275 current privileged users at six DECCs. DECC St. Louis was able to provided all 45 SAARs requested and five DECCs were unable to prove existence of 52 access request forms.

- DECC Columbus - 1 of 45 users
- DECC Mechanicsburg - 23 of 45 users
- DECC Montgomery - 11 of 48 users
- DECC Ogden - 10 of 47 users
- DECC Oklahoma City - 7 of 45 users

Site management was unable to determine whether the missing SAARs were lost or never created. From the 223 access forms that we obtained, we identified missing signatures and inconsistent level of access.

Authorizing Signatures. Six of the 223 SAARs did not have appropriate authorization signatures. The Handbook requires the security manager to validate and confirm that the user has the proper level of clearance for the requested access privilege. DECC Ogden had four access forms without security manager's signature certifying that the users had appropriate clearance for the requested access. DECCs Montgomery and St. Louis each had one access form without authorization signatures for the supervisor and the security manager. Additionally, CS did not maintain a list of authorized supervisors who could approve access forms and ensure that appropriate signatures were obtained prior to granting user access. Without complete and properly authorized access request forms, CS has little assurance that the access granted is consistent with the user's job responsibilities.

Level of Access. Thirty-five of the 223 access forms did not accurately reflect the user's level of access. DECC Ogden had 29 user accounts that did not match the authorized level of access on the SAARs. DECC Montgomery had six SAARs that did not contain the system name. Additionally, DECCs Columbus, Montgomery, Ogden, and St. Louis did not grant mainframe access based on established access profiles. Without accurate access request forms, CS cannot confirm that user privileges are consistent with user's job responsibilities and that user access is granted based on the principles of least privilege.

Account Termination. The Handbook states that the supervisor is responsible for the deletion of the user when the user no longer needs the access. In addition, the Handbook states that if access is still needed for a transferred employee, the new supervisor is required to validate the need for access. Thirteen of 257 active user accounts at DECC Columbus belonged to terminated employees. Six of 224 active user accounts at DECC St. Louis belonged to terminated or transferred employees. Two of the six DECC St. Louis individuals had been out-placed through termination or retirement. The remaining four DECC St. Louis individuals transferred to other CS or DoD organizations and retained their access privileges for the new job function. However, CS did not have evidence demonstrating the need for access from their new supervisors.

Account Management Guidance

The Handbook did not provide specific guidance on some key aspects of account management, which resulted in inconsistent procedures across CS sites. Specifically, CS did not have standard processes for conducting periodic review of user accounts, access removal, and emergency and temporary accounts.

Periodic Review. CS had no process in place to ensure periodic reviews of systems access, including privileged access, to ensure that the concept of least privilege is maintained. DoD Instruction 8500.2 requires that IAM tracks privileged role assignments; however, the Handbook did not provide guidance on how this should be accomplished. DECCs Columbus, Mechanicsburg, Montgomery, and St. Louis did not always track privileged accounts. Additionally, CS could not easily identify the number and name of systems to the responsible system administrators.

The National Institute of Standards and Technology (NIST), Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," September 1996, establishes the necessity of periodically reviewing user accounts on a system to help ensure that appropriate authorizations are received and appropriate levels of access are maintained. DECC Oklahoma City did not have a regular process to review accounts for the Tandem mainframes to comply with the Tandem STIG. For example, section 5.6 of the Tandem STIG requires that database management tools only be granted on an as-needed basis, and the three Tandem environments we reviewed did not have a regular process to periodically review and clean-up user database files when employee status changed. Periodic revalidation of user accounts helps to ensure that the concept of least privilege is maintained. Without a periodic review of user access, CS increases the risk that initial access granted to an employee or contractor will not remain appropriate in the event that individual job responsibilities and employment status change.

Access Removal. While the Handbook requires that all government and contractor personnel receive a termination briefing and execute a clearance form (DISA Form 533) when departing the organization, or when access is no longer required, this was not consistently applied. CS had not developed formal, standard out-processing procedures to ensure that access was removed at the time of termination or transfer. DECCs Columbus and Oklahoma City had their own procedures for out-processing. DECCs Montgomery, Ogden, and St. Louis had not developed and documented formal out-processing procedures for government and contractor employees leaving the facility; however, each DECC had an out-processing checklist[2]. DECC Oklahoma City inconsistently administered the out-processing of its terminated employees and contractors. Of the 44 terminated employees selected at DECC Oklahoma City, 29 terminated employees did not complete the site's termination checklist. In addition, none of these sites had effective procedures to delete or update systems access for terminated and transferred users. Standard out-processing procedures for terminated and

[2] Testing was not conducted at DECC Mechanicsburg.

transferred employees and contractors would help CS control the logical security of CS systems.

Emergency and Temporary Access. CS had not established a standard process on requesting, authorizing, and granting emergency and temporary access. The Handbook only provides recommended procedures for handling of maintenance accounts. For example, DECC Mechanicsburg did not have policies and procedures in place for the creation and maintenance of emergency user accounts, and it did not always maintain records of recently granted emergency or temporary remote access. DECC Oklahoma City did not log emergency access or remove accounts upon completion. Specific guidance and a standard process on emergency and temporary access would help to ensure that only authorized changes are performed during emergency and temporary access and that granted access is properly documented.

Recommendations and Management Comments

B. We recommend that the Director, Center for Computing Services:

1. Verify that all access request forms have been completed, properly authorized, and reflect current authorized system access for each user account.

Management Comments. The Director, CS, concurred and stated CS implemented Privileged Attribute and Access Policy and Procedures (CSD 06-05) in November 2005 and the draft Handbook, released February 2006, that address the access request form and specifies validation of access to occur annually.

2. Establish standard account management guidance, in accordance with DoD policy, to be used across entity sites, to include:

a. Procedures for requesting, authorizing, and granting access for systems for both usual and temporary and emergency access.

Management Comments. The Director, CS, concurred and stated CS implemented Privileged Attribute and Access Policy and Procedures (CSD 06-05) in November 2005 and the draft Handbook, released February 2006, that address the access request form and specifies validation of access to occur annually and that temporary and emergency access will be immediately removed from the system when the emergency event has been corrected.

b. Standards for out-processing and transferring employees and contractors, including confirmation that all access has been removed.

Management Comments. The Director, CS, concurred and stated CS established standards for out-processing and transferring employees and contractors including confirmation that all access has been removed. Personnel Out-Processing Checklist, DISA Computing Services Instruction CSD 06-14 went in effect in February 2006.

c. A process for the Information Assurance Manager to adequately track privileged access in accordance with DoD policy.

Management Comments. The Director, CS, concurred and stated CS established a process for the IAM to adequately track privileged access in accordance with DoD policy. This process is covered in the release of the draft Handbook dated February 27, 2006 and CS Privileged Attribute and Access Policy and Procedures (CSD 06-05) issued in November 2005.

d. The frequency and process for reviewing systems access, both privileged and non-privileged users accounts.

Management Comments. The Director, CS, concurred and stated CS implemented Privileged Attribute and Access Policy and Procedures (CSD 06-05). This policy addresses the frequency and process for reviewing system access annually. The policy has been in effect since November 2005.

e. Standards for documenting temporary and emergency access.

Management Comments. The Director, CS, concurred and stated CS has established procedures for documenting access for temporary and emergency access in accordance with the draft Handbook released in February 2006.

C. Audit Trails

General controls over audit trails were not effective. The controls were not effective because CS had not implemented controls that fully complied with current DoD policies. Audit trails were not regularly monitored and analyzed for inappropriate or unusual activities and audit trails were not maintained for the required amount of time. In addition, the required permissions settings were not consistently set to protect the audit trails. The lack of adequate audit trails and regular monitoring increases the risk that unauthorized user activities may not be detected in a timely manner or not detected at all. Furthermore, audit logs may not be available for proper analysis in a security incident investigation.

Audit Trail Controls

CS had not implemented effective procedures for monitoring and maintaining audit trails. Audit trails are critical in detecting unauthorized or fraudulent activities. The lack of regular monitoring of audit trails may hinder CS from effectively securing its systems against security and infrastructure vulnerabilities. Appropriate access control software should be used to maintain an audit trail to determine how, when, and by whom specific activities were performed. In addition, audit trails should be maintained and protected. Incorrect audit log settings may allow unauthorized modifications to the log files.

Review of Audit Trails

CS did not regularly monitor and analyze audit trails. While system logs were automatically generated by the various platforms at the DECCs, information captured by the system logs was voluminous. The size of the log files prevented the IA Officers (IAOs) from effectively monitoring and reviewing information regarding unauthorized attempts. In addition, CS did not have a consistent methodology for generating an audit trail based on unusual or inappropriate activity flagged by the system logs.

CS did not effectively monitor or review the audit trails to ensure compliance with DoD and CS requirements. DoD Instruction 8500.2 requires that audit records from all available sources be regularly reviewed for indications of inappropriate or unusual activities. In addition, the Handbook requires that the IAO review the audit trails on a weekly basis at a minimum. DECCs Mechanicsburg, Montgomery, Ogden, and St. Louis did not perform effective review of the audit logs for their systems, because CS did not provide or communicate standard procedures across the DECCs.

Additionally, CS did not have an effective mechanism for monitoring audit trails to detect unauthorized attempts to gain system access, or to detect unauthorized changes made to system software. DoD Instruction 8500.2 requires that tools be available for the review of audit records and for report generation. CS had not provided a standard set of auditing tools for the sites to produce formal, easy to use reports from audit logs.

The lack of adequate monitoring and analyzing audit trails increases the risk that unauthorized user activity may not be detected or detected in a timely manner. Effective review of the reports from audit logs facilitates the analysis of logged events and can help to ensure a timely response to security incidents. Otherwise, unauthorized or inappropriate use of CS resources may not be detected and investigated in a timely manner.

Audit Trail Retention

CS did not consistently maintain audit trails for the amount of time required by DoD and CS policies. DoD Instruction 8500.2 requires that the audit records be backed up at least once a week onto a different system or media other than the system being audited, and that audit records be retained for at least one year. The Handbook also requires the audit trails be maintained for one year.

DECCs Montgomery, Ogden, and Columbus did not comply with the DoD record retention requirements.

- DECC Montgomery did not have designated audit servers.
- DECC Ogden did not always send the security and audit logs to its audit server.
- DECCs Montgomery and Ogden did not consistently retain audit records for all platforms for at least one year.
- DECC Columbus archived its audit logs every 14 days and recycled the archive media every 100 days.
- DECC Montgomery only maintained its UNIX audit logs for 24 hours, and then deleted them.
- DECC Ogden, in some cases, deleted its Windows audit logs when the files became too voluminous.

As a result, audit logs were frequently deleted and were not protected from unauthorized access, modification, or deletion. Audit logs should be secured from potential deletion or manipulation to help ensure that they are available for review and analysis in the event of a security incident. Backing up audit logs to a separate system helps to protect the logs from unauthorized access, modification or deletion.

Audit Log Settings

CS did not consistently have the required permissions settings to protect the audit data files. UNIX STIG requires the auditing systems to capture events like, but not limited to, logon and logout, unauthorized access attempts, use of privileged commands, systems administration actions, and security personnel actions. Twenty-nine of 49 UNIX devices tested failed to capture the required events.

DoD Instruction 8500.2 requires that the contents of audit trails are protected against unauthorized access, modification, or deletion. UNIX STIG also requires that audit data files have the permission of 640 or more restrictive. A permission of 640 allows the file creator or file owner with the read and write permission, the file owner’s group with the read permission, and everyone else on the system with no permission. Ten of the 49 UNIX devices tested had audit data files with permissions less restrictive than 640.

Incorrect audit log settings may cause the audit systems not to capture sufficient information, or the information may be altered or deleted. As a result, unauthorized access or inappropriate activities on the CS systems may not be detected, investigated, or corrected.

Recommendations, Management Comments, and Audit Response

As a result of management comments, we redirected recommendation C.1.a from the Director, CS to the Chief, FSO and renumbered recommendation C.1.a to C.2.

C.1. We recommend that the Director, Center for Computing Services implement consistent procedures across the entity to create, monitor and review, protect, and maintain CS system audit trails to comply with the requirements of DoD Instruction 8500.2 and Security Technical Implementation Guides to include:

a. Backup audit trails to a different system or media.

b. Maintain audit trails for at least one year.

c. Configure permission setting correctly to protect the audit trail data.

Management Comments. The Director, CS, concurred and stated CS will follow the minimal auditing requirement document developed in March 2006 by the FSO. This guidance will be followed until a standard set of auditing tools is provided by the FSO.

C.2. We recommend that the Chief, Field Security Operations, implement consistent procedures across the entity to create, monitor and review, protect, and maintain CS system audit trails to comply with the

requirements of DoD Instruction 8500.2 and Security Technical Implementation Guides to provide a standard set of auditing tools.

Management Comments. The Chief, FSO, concurred and stated there is an Enterprise Wide Solutions Steering Group initiative this year to acquire an audit capability, referred to as a Tier III Security Incident Manager. The acquisition for the solution is planned to begin in late FY 2007. The solution will be a DoD level initiative and DISA plans to leverage the Tier III Security Incident Manager solution once it becomes available to DoD.

Audit Response. The implementation of auditing tools within DISA is dependant on the successful completion of the acquisition strategy; therefore we consider management comments as responsive. We request that DISA provide updates on the scheduled implementation as part of their normal activity reports to the DoD, Office of the Inspector General.

D. Contingency Plans

General controls over contingency plans were not effective and did not fully comply with DoD requirements. The controls were not effective because CS did not have adequate management controls over developing, maintaining, and testing contingency plans. CS did not:

- have a comprehensive entity-wide contingency plan;
- have site-specific contingency plans for 7 of 16 DECCs and did not have current, comprehensive, or approved contingency plans for the remaining 9 sites; and
- perform regular, comprehensive contingency plans testing at all DECCs.

Without current, comprehensive, and approved contingency plans, CS is at risk of not being able to process, retrieve, and protect information maintained electronically in the event of service interruptions. The absence of periodic comprehensive testing increases the risk that CS personnel will not be aware of the appropriate actions or the procedures to perform to resume processing in a timely manner.

Continuity of Operations Plans

General controls over contingency plans, known as continuity of operations plans (COOPs), were not effective and did not fully comply with DoD requirements. DoD Instruction 8500.2 requires that a plan exists that provides for the resumption of mission or business essential functions within 24 hours activation and that the plans are exercised annually. The COOPs serve to restore critical applications in the event that the usual facilities are significantly damaged or cannot be accessed. The COOPs should be clearly documented to reflect the risks and operational priorities that the entity has identified, and updated to reflect current operations. The COOPs include business recovery plans, system contingency plans, facility recovery plans, and plan acceptance. Each entity should have an entity-wide COOP supplemented by site-specific COOPs. In addition, the COOPs should be tested through scheduled exercises and drills. CS did not have effective controls established to ensure that contingency plans were adequately developed, maintained, tested, and operating effectively to fully comply with Federal and DoD requirements.

Entity-Wide COOP

CS had not developed and implemented a comprehensive entity-wide COOP. With the CS transformation, DECCs are becoming centrally managed and more interdependent of each other. Therefore, CS needs an entity-wide COOP, supplemented by the site-specific COOPs to ensure timely recovery in the event of a service interruption. The entity-wide COOP should address, at the entity level, the mission or business essential functions for priority restoration planning. Without an entity-wide COOP that integrates the site COOPs, CS may not be able to effectively protect information resources and effectively minimize risk related to unplanned interruptions. In addition, CS may not be able to recover and restore critical applications and resume processing in the event of an emergency at the enterprise level.

Site-Specific COOP

CS did not have site-specific COOPs for 7 of the 16 DECCs, and the site-specific COOPs were not current, comprehensive, or approved for the remaining 9 DECCs. Each DECC needs its own COOP to address the specific issues on the unique operational environments of each facility. For example, SMCs would require more comprehensive plans than PEs and ISCs. DoD Instruction 8500.2 requires that a COOP exists to provide for the resumption of mission or business essential functions within 24 hours activation. As a result, the COOPs need to clearly identify mission and business essential functions for priority restoration planning, along with all supporting assets, be updated to reflect the current operations, and be approved by management.

Plan Documentation. DECCs Dayton, Denver, Huntsville, Jacksonville, Norfolk, San Diego, and Warner Robins had not developed site-specific COOPs; and DECCs Chambersburg, Mechanicsburg, Montgomery, Oklahoma City, Rock Island, San Antonio, and St. Louis did not have comprehensive or current COOPs. For example, the COOP for DECC Montgomery did not include details on voice telecommunication needs, backup personnel for key individuals, and manual processing procedures for customer activities. In addition, the COOP for DECC St. Louis did not reflect changes occurred during the year, and personnel from DECC St. Louis stated that the site COOP would become obsolete with the transformation.

Management Acceptance. CS did not have a process in place to ensure that local site management had formally reviewed and accepted the site-specific COOP. CS has established a group at the Rocky Mountain Center, Denver, CO, that is responsible for reviewing and approving the individual CS site COOPs. DECCs Chambersburg, Columbus, Montgomery, Ogden, Oklahoma City, Rock Island, and St. Louis did not have formal management review and acceptance of their COOPs. Management acceptance of the COOP is essential to ensure that individuals involved in executing a COOP understand their responsibilities and that they are aware of the procedures to effectively restore operations.

An organization needs a comprehensive and detailed plan to fully recover key applications and support systems. A current COOP is an absolute essential to an organization experiencing changes to its business, personnel, and processing structure. The ability for CS to react efficiently and effectively in service interruption relies heavily on comprehensive and current COOPs. Therefore, CS needs to have comprehensive and current site-specific COOPs and management acceptance of the COOPs to ensure adequate recovery procedures in the event of an emergency.

Periodic Testing

CS did not perform regular, comprehensive COOP testing to include the recovery of CS operations at all DECCs as required by DoD regulation. For the nine DECCs with site-specific COOPs, none of the DECCs performed comprehensive testing of individual site COOPs. DECCs Chambersburg, Columbus, Mechanicsburg, Montgomery, Ogden, Oklahoma City, Rock Island, San Diego, and St. Louis were unable to demonstrate that COOP testing was ever conducted, or indicated that testing had not been performed in over a year. DoD Instruction 8500.2 requires the performance of annual COOP testing through scheduled exercises and drills.

COOP testing helps to ensure that recovery plans remain current and that they can provide effective recovery guidance in the event of an emergency. Comprehensive testing on a regular basis helps to ensure that site personnel understand and are adequately prepared to successfully perform recovery procedures in the event of an actual service interruption. Annual testing helps to ensure that site personnel are familiar with the platform and technologies to effectively recover systems as necessary. Without regular and comprehensive COOP testing across CS platforms and customer applications, CS cannot ensure that its COOP procedures will support a timely recovery in the event of an emergency.

Recommendations and Management Comments

D. We recommend that the Director, Center for Computing Services:

1. Create a comprehensive entity-wide Continuity of Operations Plan.

Management Comments. The Director, CS, concurred and stated CS has created a comprehensive COOP for all sites as of February 2006.

2. Create or update site specific Continuity of Operations Plans to ensure they reflect the current organizational structure, and provide adequate recovery of designated key systems; and integrate these plans into the entity-wide Continuity of Operations Plan.

Management Comments. The Director, CS, concurred and stated CS has created and updated site specific COOPs to ensure they reflect the current organizational structure, and provide adequate recovery of designated key systems; and integrated these plans into the entity-wide COOP completed as of February 2006.

3. Establish a standard process to:

a. Review Continuity of Operations Plans to ensure they are comprehensive and complete.

b. Track and monitor changes and perform annual updates.

c. Require formal and documented management review and acceptance of the plans at the Defense Enterprise Computing Center level.

d. Submit site plans to Rocky Mountain Center, Denver, Colorado for final review and approval.

Management Comments. The Director, CS, concurred, and stated CS has established a Concept of Operations document that:

- ensures the process of reviewing the enterprise COOP is comprehensive and complete;
- ensures the tracking and monitoring of changes, and annual updates are performed; and
- requires formal and documented management review and acceptance of each sites' plan at the DECC Service level and the plans are maintained at the Tech Center in Denver, Colorado.

Concept of Operations has been in effect as of August 2005.

4. Establish and implement standard policies and procedures for performing annual comprehensive Continuity of Operations Plans testing. Document the results and lessons learned.

Management Comments. The Director, CS, concurred and stated CS has established a Concept of Operations document, which requires testing and documenting annual comprehensive COOPs. CS is planning on conducting a test of the plan no later than August 2006.

E. Data Backup and Off-Site Storage

Controls over data backup and off-site storage were not in place and did not fully comply with DoD policy. This occurred because CS had not developed adequate management controls to effectively manage data backups and off-site storage. Thirteen of 16 sites did not have adequate procedures to manage data backups and 9 of 16 off-sites facilities did not have adequate physical and environmental controls. The lack of adequate guidance for data backup and storage could limit the ability for CS to restore operations and process essential data in a timely manner.

Backup and Storage

CS had not implemented effective controls over data backup and off-site storage to ensure compliance with DoD and CS policy. CS had not developed, implemented, and tested backup procedures to help ensure the integrity of data and the timely recovery of data in the event of a service interruption. In addition, CS had not ensured that all off-site storage facilities could provide adequate physical and environmental controls to protect data from physical damage, unauthorized access, and loss.

DoD Instruction 8500.2 requires that data backup be performed daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with the MAC and confidentiality level assigned. The instruction also requires that backup copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocated with the operational software.

Additionally, DISA Instruction 360-225-08, “Magnetic Tape Backup and Storage by DECCs and DECC Detachments,” requires:

- Documented procedures for identifying backups, as well as procedures for rotating and retaining backups;

- The most current cycle of full volume backup tapes and the previous copy for each system be removed to an off-site storage facility at least weekly;

- Off-site storage arrangements to include established procedures for managing and controlling the rotation of backups;

- The off-site recovery facility to be a minimum of 25 miles from CS processing sites;

- Off-site storage arrangements which include appropriate physical controls, including a list of pre-identified personnel who have authorized access to the off-site facility; and

- Environmental controls, including controls for temperature, humidity, fire protection, and electrical power backup.

Finally, NIST 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, states that backup tapes should be tested regularly to ensure that data are being stored correctly and that the files may be retrieved without errors or lost data. Additionally, the backup tapes should be tested at the alternate site, if applicable, to ensure that the off-site facility supports the same backup configuration that the DECC has implemented.

Backup Procedures

CS had not developed adequate procedures to effectively manage data backups in the event of a service interruption. Thirteen of 16 sites did not have adequate procedures to manage data backups, which could negatively impact the handling of backup data. For example:

- DECCs Dayton, Denver, Jacksonville, Mechanicsburg, and Rock Island did not have formal, comprehensive standard operating procedures for managing data backups.

- DECCs Columbus, Dayton, Huntsville, Mechanicsburg, and Warner Robins did not appropriately mark and catalogue the data backup tapes to ensure effective identification of data to facilitate recovery. For example, DECC Mechanicsburg did not have a unique numbering system for storing and pulling backup tapes, and DECCs Columbus and Huntsville did not produce an inventory listing or log of on-site and off-site tapes. Additionally, the DECC Huntsville off-site facility had unorganized data backup tapes, and the DECCs Dayton and Warner Robins off-site facilities had tape containers that were unaccounted for.

- DECCs Chambersburg, Mechanicsburg, Montgomery, Norfolk, Rock Island, San Antonio, and Warner Robins did not regularly test the backup tapes to ensure that the tapes could be used to recover programs, data, or operating systems.

- Physical controls over the backup tapes were not consistently maintained when transporting backup tapes to the off-site location. For example, DECCs Huntsville and Mechanicsburg transported their backup tapes to the off-site facility in unsecured containers by personal vehicles.

- DECC Jacksonville did not store its backup copies of the operating system and other critical software in a fireproof container or at an off-site facility.

- DECCs Chambersburg, Dayton, Denver, Huntsville, Jacksonville, Mechanicsburg, Norfolk, Rock Island, San Antonio, San Diego, and

Warner Robins, did not utilize off-site facilities to store copies of key documents like system and application documentation and COOP plans.

- DECCs Jacksonville, Rock Island, and San Antonio did not consistently rotate their weekly data backup tapes to the off-site facilities.

In the absence of procedures to ensure comprehensive backups of all production data, the risk is increased that CS cannot recover all production systems and data in the event of an emergency.

Off-Site Facility

CS had not ensured that off-site storage facilities could provide adequate physical and environmental controls to protect its data from physical damage, unauthorized access, and loss. Nine of 16 off-sites facilities did not have adequate physical and environmental controls. For example,

- Off-site facilities for DECCs Huntsville, Oklahoma City, and Warner Robins were located less than 25 miles away.

- DECCs Huntsville, Montgomery, St. Louis, and Warner Robins off-site facilities did not maintain a listing of personnel who were authorized to access CS data at the off-site facilities.

- DECC Columbus did not require visitors to the off-site facility to sign into a visitor log.

- Off-site facilities for DECCs Chambersburg, Jacksonville, San Antonio, and Warner Robins did not have a backup power supply.

- Off-site facility for DECC Columbus did not have the acceptable temperature and humidity range.

In the absence of procedures to ensure that off-site storage facilities can provide adequate controls to protect its data from physical damage, unauthorized access, and loss, the risk is increased that CS cannot recover all production systems and data in the event of an emergency.

An entity takes a number of steps to prevent or minimize the damage to automated operations that can occur from unexpected events. Implementing thorough backup procedures and installing environmental controls are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters. An entity should regularly backup and securely store backup copies at an off-site location. The off-site location should be far enough from the primary location that it will not be impaired by the same events, such as fires, storms, and electrical power outages. The off-site location should be protected from unauthorized access and environmental hazards.

Recommendations and Management Comments

E. We recommend that the Director, Center for Computing Services:

1. Develop, implement, and test consistent data backup policies and procedures across all entity sites. These policies and procedures should include:

a. A process for appropriately marking and cataloging recovery data.

Management Comments. The Director, CS, concurred and stated the CS has established a process for appropriately marking and cataloging recovery data in accordance with the draft Handbook released in February 2006.

b. A process to periodically test data backups to ensure timely recovery in the event of a service interruption or emergency.

Management Comments. The Director, CS, concurred and stated the CS uses Veritas Tape backup system, which does a bit for bit test of data that is backed up for all systems. CS has established a process to periodically test data backups to ensure timely recovery in the event of a service interruption or emergency for customers that provide backup servers or logical partitions in accordance with the Service Level Agreement (SLA).

c. Consistent physical control over backup tapes when transporting to and from the off-site facility.

Management Comments. The Director, CS, concurred and stated CS has implemented CS Letter of Instruction 06-01, dated October 2005, directing the sites to have consistent physical control over backup tapes while the backup tapes are being transported to and from the off-site storage facility.

d. Standards for securing and storing critical software on-site when copies are not maintained at the off-site facility.

Management Comments. The Director, CS, concurred and stated CS has implemented CS Letter of Instruction 06-01, dated October 2005, providing guidance on securing and storing critical software on-site when copies are not maintained at the off-site facility.

e. Requirements for storing copies of key documentation at the off-site facility.

Management Comments. The Director, CS, concurred and stated CS has implemented CS Letter of Instruction 06-01, dated October 2005, providing guidance on storing copies of key documentation at the off-site facility.

f. Requirements for rotating the weekly data backup tapes to the off-site facility.

Management Comments. The Director, CS, concurred and stated CS has implemented CS Letter of Instruction 06-01, dated October 2005, requiring the sites to rotate the weekly data backup tapes to the off-site facility.

2. Implement procedures to verify that proper physical and environmental controls, which include minimum distance requirements, lists of authorized personnel, visitor logs, backup power, and temperature and humidity controls are in place at the off-site facility.

Management Comments. The Director, CS, concurred and stated CS implemented CS Letter of Instruction 06-01 in October 2005. This policy directs that proper physical and environmental controls, which include minimum distance requirements, lists of authorized personnel, visitor logs, backup power, and temperature and humidity controls are in place at the off-site facility.

F. Safeguarding Assets

The physical and environmental controls at the DECCs did not adequately safeguard equipment and fully comply with DoD and DISA policy. This occurred because CS management did not effectively implement management controls that address the safeguarding of data and equipment. CS had:

- inadequate physical security controls and procedures at the DECCs,
- inadequate environmental controls at 12 DECCs,
- inadequate hardware maintenance policies and procedures, and
- inadequate controls over sanitation of decommissioned equipment.

Without adequate procedures implemented to protect data and equipment, the risk of unauthorized access, modification, destruction, and disclosure of data and CS resources is increased. Furthermore, without effective environmental controls, the risk for potential loss of data and CS resources is increased.

Safeguarding Data and Equipment

CS had not implemented sufficient physical and environmental controls to adequately safeguard equipment and to fully comply with DoD and DISA policy. DoD Instruction 8500.2 establishes the basic requirements for safeguarding data and equipment through effective implementation of physical and environmental controls. The Instruction requires effective controls to restrict physical access into computing facilities processing sensitive information to only authorized personnel who have a need to be onsite. The DISA Instruction 360-225-08 requires the DECCs and off-site storage facilities to have adequate environmental controls related to temperature, humidity, and fire protection.

CS management did not implement policies and procedures that address the safeguarding of data and equipment to fully comply with DoD Instruction 8500.2 and the Handbook. Specifically:

- CS had inadequate controls and procedures over physical security around the DECCs.
- CS had inadequate environmental controls across 12 DECCs.
- CS did not implement procedures to ensure that hardware received scheduled maintenance, SLAs were documented with vendors, and that site personnel responsible for managing hardware were not aware of these SLAs and the level of services provided.
- DECCs Mechanicsburg and St. Louis did not maintain evidence for sanitizing decommissioned equipment.

Physical Security

CS had not established adequate physical security around the DECCs. Controls surrounding entrances and exits at DECCs Dayton, Huntsville, Montgomery, Norfolk, Rock Island, and San Diego did not comply with DoD and CS requirements. Specifically, computer room doors opened outwards and hinges were not secured, monitoring devices were not in place to monitor access to the building or computer room, and personnel were "piggy-backing" into the facility.

Procedures did not consistently exist for granting and revoking physical access to the computer room. For example, a formal process did not exist for notification of change in personnel positions and modification of access at DECCs Chambersburg, Montgomery, San Diego, and Warner Robins. In addition, some physical access request forms were missing at DECC Chambersburg, Columbus, Dayton, Ogden, San Antonio, and San Diego. Furthermore, some physical access request forms had incomplete details to determine the appropriate clearance level to grant at DECCs Huntsville, Jacksonville, Montgomery, and San Antonio.

The Handbook requires records to show the current location and custody of each key; annual inventories of issued keys; semi-annual inventories of unissued keys; and a key listing that identifies each key within the key box by slot. Controls over keys were not adequate at DECCs Dayton, Denver, Montgomery, Norfolk, Ogden, and Warner Robins. For example, key logbooks did not always exist, keys within the key lock box were not always labeled, an inventory of keys did not always exist, and unissued keys and other access control devices were not always controlled.

Facility penetration testing procedures were not developed or conducted at DECCs Chambersburg, Columbus, Denver, Huntsville, Jacksonville, Montgomery, Norfolk, Oklahoma City, Rock Island, San Antonio, and Warner Robins to ensure that adequate physical security was implemented around the facilities. In addition, DECC Dayton did not have appropriate labeling and protective covers for emergency electricity shut-off panic buttons.

Weak physical security controls at the DECCs increase the vulnerability of external threats as unauthorized individuals could gain entry to the computer room and modify, disclose, damage, or destroy equipment and data.

Environmental controls

CS had not implemented adequate environmental controls at 12 of 16 DECCs to ensure compliance with DoD Instruction 8500.2 and DISA Instruction 360-225-08. Adequate environmental controls were not in place for DECCs. Specifically, four DECCs did not have adequate controls over fire suppression. Hand-held fire extinguishers in the maintenance machine room at DECC Montgomery had not been inspected since 2002 or did not have inspection tags; fire extinguishers at DECC San Antonio had not been inspected within the last year, and the facility had not had a Fire Marshall inspection in over a year.

Fire alarms at DECC Denver did not automatically notify the fire department. Fire sprinkler system was not visible in all rooms of the DECC Chambersburg facility.

Nine DECCs did not have adequate controls over water detection. Water detection sensors were either not present or inoperable under the raised floor at DECCs Dayton, Denver, Huntsville, Mechanicsburg, Ogden, Oklahoma City, St. Louis, and Warner Robins. Humidity protection and monitoring were not present throughout the facility at DECC Montgomery. As a result of inoperable water detection sensors, data backup tapes were damaged by a water leak in the tape vault at DECC Ogden. Blue prints detailing the environmental controls for DECC Montgomery were not updated since the 1970's and did not reflect the current state of plumbing lines at the site.

Six DECCs did not have adequate controls over backup power. There was no evidence to support generator testing at DECCs Dayton, Jacksonville, and Mechanicsburg. DECC San Antonio did not have adequate uninterrupted power supply; of the three generators at DECC San Antonio, one was inoperable and one was considered unreliable. No protective clothing or bath was available to employees in the battery room at DECCs Montgomery and Rock Island.

Eleven DECCs did not have adequate employee training. Facility employees had not consistently received initial or periodic training in the operations of environmental controls at DECCs Dayton, Huntsville, Jacksonville, Montgomery, Mechanicsburg, Norfolk, Ogden, San, Antonio, San Diego, and Warner Robins. No formal policy or procedure existed to prohibit food or drinks in the computer rooms at DECCs Dayton, Huntsville, Jacksonville, Mechanicsburg, Ogden, St. Louis, and Warner Robins.

The lack of effective environmental controls at the DECCs increases the risk of loss, or damage to, data and CS computing resources. In addition, the lack of periodic testing of environmental controls increases the risk that environmental controls will not operate as necessary in the event they are needed.

Hardware Maintenance

CS had not implemented adequate hardware maintenance policies and procedures to prevent or minimize the impact of unexpected interruptions. Specifically, logs documenting scheduled and unscheduled site maintenance were not maintained at DECCs Dayton, Denver, Huntsville, Jacksonville, Norfolk, San Antonio, and San Diego. Although Remedy, a trouble ticket tracking application, was established to be used across CS sites for this purpose, this system was not consistently being used to log system maintenance and approvals.

Because the responsibility for SLAs had transitioned to Business Management Centers in Chambersburg and Denver, site personnel responsible for managing hardware were not necessarily made aware of SLAs and the level of services provided by CS sites. Facilities managers for DECCs Chambersburg, Dayton, Denver, Huntsville, Mechanicsburg, and San Diego were not aware of support services and spare parts included in contractual agreements for their respective sites, which are maintained by vendors. Because the facility site managers were not aware of the support services covered by the SLAs, vendor maintenance and other support services could not be ensured and could negatively impact the availability of CS systems and resources.

The lack of regular hardware maintenance increases the potential for hardware failure and a resulting negative impact on customer services. The risk of potential loss of customer services is augmented by the lack of spare parts and equipment that would be needed in the event of an emergency.

Sanitization of Equipment

DECCs Mechanicsburg and St. Louis did not maintain evidence for sanitizing decommissioned equipment. For example, DECC Mechanicsburg placed an orange sticker on the hardware once it has gone through the process; however, in this case, evidence supporting the completion of the clearing and sanitizing process was not maintained. DECC St. Louis did not maintain documentation that any hardware sanitization process had been followed before disposing of equipment. According to DoD Instruction 8500.2, and DoD 5200.1-Regulation and Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001, all documents, equipment, and machine-readable media containing sensitive data must be cleared and sanitized before being released outside of DoD. Without a record to certify that the hardware has been overwritten, degaussed or destroyed, there is no assurance that equipment containing sensitive information has gone through this process before being released outside DoD. This could result in unauthorized individuals obtaining sensitive DoD information and data.

Recommendations and Management Comments

F. We recommend that the Director, Center for Computing Services:

1. Implement procedures to ensure physical controls of the facilities meet DoD and Defense Information Systems Agency policies.

Management Comments. The Director, CS, concurred and stated the CS, Operations Chief has directed that all site directors post signs stating that piggy-backing into the facility computer rooms is not allowed. Computer room doors at the specified sites have been corrected to meet Handbook requirements, except for PE San Diego. PE San Diego is a Navy tenant and has submitted a request to Navy facilities requesting the entrance door to the computer room be modified to meet Handbook requirements. CS established standards for out-processing and transferring employees and contractors including confirmation that all access has been removed. Personnel Out-Processing Checklist, DISA Computing Services Instruction CSD 06-14 went in effect in February 2006.

2. Review the site environmental controls to ensure they are adequately protecting the computing facility environment and meet DoD and Defense Information Systems Agency policies.

Management Comments. The Director, CS, concurred and stated the CS, Operations Chief has directed that all site directors ensure that the sites review their environmental controls and that they ensure compliance with the Handbook.

3. Implement procedures to ensure that maintenance employees received the required training.

Management Comments. The Director, CS, concurred and stated CS implemented CSD policy 06-17 in March 2006 to define roles and responsibilities of employees in the maintenance process. In addition, the maintenance training plan will be developed by September 30, 2006.

4. Implement procedures to ensure that hardware receives scheduled maintenance and that the maintenance has been documented.

Management Comments. The Director, CS, concurred and stated CS implemented CSD policy 06-17 in March 2006 defining the maintenance procedures.

5. Develop procedures to ensure that site facility managers are provided with appropriate information on the support services covered by Service Level Agreements to enable them to perform necessary maintenance on site resources.

Management Comments. The Director, CS, concurred and stated CS implemented CSD policy 06-17 in March 2006 defining the maintenance procedures.

6. Implement procedures to document compliance with the requirements of DoD Instruction 8500.2 for clearing and sanitizing decommissioned assets.

Management Comments. The Director, CS, concurred and stated CS has updated the Handbook, draft released in February 2006, to document compliance with the requirements of DoD Instruction 8500.2 for clearing and sanitizing decommissioned assets.

G. Configuration Management

General controls over configuration management were not effective. The controls were not effective because CS management had not implemented standard and effective configuration management policies and procedures across sites to ensure compliance with DoD policy. CS did not implement standard policies and procedures to be applied across sites to review, approve, and track configuration changes throughout the change control cycle, from the initial request through implementation and closeout and personnel involved in the configuration management process had not consistently participated in related training. The lack of a standardized configuration management program could lead to unauthorized and potentially detrimental modifications to customer applications, negatively impacting business operations and the CS infrastructure.

Configuration Management Program

CS management had not implemented standard configuration management (CM) policies and procedures across sites to ensure compliance with DoD policy. CS did not have an effective CM program to manage configuration changes to its computing resources, as required by DoD Instruction 8500.2. DoD Instruction 8500.2 requires a CM process to be implemented that includes the following:

- Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation;

- A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems;

- A testing process to verify proposed configuration changes prior to implementation in the operational environment; and

- A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.

Configuration change controls for software development are necessary to prevent unauthorized programs, or inappropriate modifications to authorized programs, from being implemented. Configuration change controls should include review and approval of application configuration change requests and technical system features to assure that configuration changes are executed by authorized personnel and properly implemented.

Configuration Management Policies and Procedures

CS management did not ensure that CM processing procedures were documented and personnel involved in the CM process had not consistently participated in related training, as required by DoD Instruction 8500.2. The CS CM process is the responsibility of the CS Executive Software Configuration Control Board, with local Configuration Control Boards (CCBs) established at individual sites. The CCBs take final action on all changes made to customer applications, hardware, operating system and utility software, and communications and networks in the CS environment. Specifically, CS:

- Did not implement standard CM policies and procedures applied across sites to review, approve, and track configuration changes throughout the change control cycle, from the initial request through implementation and closeout;

- Did not develop a uniform configuration change request process;

- Did not consistently use or maintain standard CM documentation across CS sites, including change requests, test plans and results, and document formal management approval;

- Did not establish procedures to ensure that all configuration changes made were authorized and appropriately implemented;

- Did not establish procedures to ensure compliance with DoD Instruction 8500.2, that prohibits the use of binary or machine executable public domain software products, shareware, and freeware; and

- Did not enforce periodic training for personnel involved in the CM process.

Configuration Management Policies and Procedures. CS had not implemented configuration management policies and procedures that were consistently applied across sites. Policies that defined change management responsibilities for all the parties involved, including CS Headquarters, Systems Support Offices (SSOs), DECCs, and customer end-users, were not developed, resulting in inconsistent processes across CS.

- DECC Montgomery had no configuration management process that tracked configuration changes to system software or customer business applications from initial request through implementation and closeout.

- While SSO Montgomery had a process for implementing configuration changes to the Enterprise Systems Management (ESM) suite of applications, it did not follow the CM process and did not maintain adequate documentation of configuration changes, including configuration change requests, test plans and results, and management approval of configuration changes.

- DECC Columbus was no longer using its CCB to review configuration changes.

- DECC Mechanicsburg had not included the IAM in the CCB to ensure that security risks were adequately addressed prior to implementing configuration changes.

The lack of implemented standardized CM management policies and procedures could lead to inconsistent processes across CS sites, resulting in potentially unauthorized modifications to operating systems managed by CS and to the applications and data supported by CS for its customers.

Configuration Change Request Mechanism. CS had not developed a uniform configuration change request process, and DECCs utilized locally managed application systems to support their processes. DoD Instruction 8500.2 requires a CM process that documents roles, responsibilities, and procedures; establishes a configuration control board to ensure security reviews and approvals for all proposed system configuration changes; implements a standard testing process; and establishes verification procedures to provide assurance that the process is properly working. The Instruction also requires a review and approval process to help prevent unauthorized programs, or inappropriate modifications to authorized programs, from being introduced. CS did not have standardization across its sites. For example:

- For six of seven Unisys platforms tested, system administrators were allowed to perform configuration changes to software applications without any formal approval. In addition, most of these configuration changes did not include a documented backup plan in the event a configuration change would need to be reversed.

- DECC Montgomery maintained listings of configuration changes made to the ESM suite of applications in its Defense Software Engineering Management System database. In addition, DECC Montgomery did not have a system dedicated to tracking CM changes.

- DECC Oklahoma City utilized the Configuration Control Tracking System to document and track software configuration changes.

- DECCs Ogden and St. Louis utilized an online Configuration Management System, a locally maintained database that tracked all configuration change requests from initial request to closeout.

- DECC Columbus did not have an effective configuration change process to track application configuration changes from approval to installation into production. In addition, DECC Columbus did not have a process to ensure that new systems and major upgrades were fully tested and authorized prior to connection to the network.

The lack of a centralized configuration change request process impairs the ability of CS to ensure that all configuration changes are uniformly reviewed and approved, and that changes are consistently tracked.

Configuration Change Request Documentation. CS was not in compliance with DoD Instruction 8500.2 requiring review and approval of application configuration change requests at five of the six DECCs tested. Standard CM documentation, including configuration change requests, test plans and results, and management approval, was not used and maintained consistently across CS sites, resulting in inconsistencies across the sites for approvals, test procedures, and test results. For example:

- DECCs Montgomery, St. Louis, and Columbus did not use a central repository of documentation to provide an audit trail for configuration changes, including initial change requests, test plans and results, customer coordination, management approval, implementation details, and documentation of user acceptance.

- While SSOs Montgomery and Mechanicsburg were responsible for testing and distributing updates and configuration changes to system software for all CS sites, DECC Columbus had made system software changes without obtaining formal approval from DECC Mechanicsburg.

- DECC Ogden had a process for submitting configuration change requests to site management for review and approval; however, the documentation and audit trail were incomplete. In addition, configuration changes had been made with no evidence of management review and approval.

Without configuration change request documentation, CS lacks a comprehensive audit trail that documents the configuration change control process, and CS cannot substantiate that all implemented configuration changes were appropriately approved.

Configuration Control Monitoring. CS did not establish procedures to ensure that all configuration changes made were authorized and appropriately implemented. DoD Instruction 8500.2 requires that only approved configuration changes be implemented by personnel authorized to perform that function. Because there was no centralized configuration change control process implemented uniformly across all sites, CS had no standard audit trail of configuration changes that could be regularly reviewed and monitored to ensure that all configuration changes made to production systems were properly implemented once approved by the CCB. Inadequate monitoring of configuration changes can lead to unauthorized or inappropriate configuration changes being made without being detected in a timely manner. Without a comprehensive process to periodically review and monitor the audit trail of configuration changes, CS cannot be certain that only authorized configuration changes to system software and applications have been introduced into the CS environment.

Public Domain Software. CS did not have adequate procedures to ensure that binary or machine executable public domain software products, shareware, and freeware were precluded from use on CS systems, as required by DoD Instruction 8500.2. At the five DECCs where public domain testing was performed, an officially approved listing of software did not exist or regular inspections of workstations were not being conducted to ensure compliance with these policies. For example, DECCs Montgomery, Oklahoma City, and Ogden understood DoD Instruction 8500.2 but had not implemented procedures to verify compliance. DECCs Columbus, Mechanicsburg, and Oklahoma City did not maintain a list of approved software to verify compliance with DoD Instruction 8500.2 on the use of public domain software. As a result, prohibited software had been installed on CS systems in DECCs Montgomery and Ogden.

The lack of regular inspection and monitoring makes it difficult for CS to ensure that all IA and related IT products installed on its systems have been configured in accordance with DoD security configuration guidelines. In addition, the risk of systems that are not appropriately secured against security and infrastructure vulnerabilities is increased due to the lack of current and complete listings of approved software necessary for daily operations; and the lack of monitoring procedures to ensure that only authorized software is installed on CS workstations.

Configuration Management Training. Personnel assigned to the CM branches at DECCs Montgomery and Ogden had not consistently participated in periodic training related to their job functions. In addition, periodic training related to CM job functions had not been provided. DoD Instruction 8500.2, requires that all personnel receive training and familiarization to help them perform their assigned IA responsibilities, including CM. Without proper and periodic training, personnel executing CM procedures may not be aware of the requisite requirements, increasing the risk that they may not follow proper procedures.

Recommendations and Management Comments

G. We recommend that the Director, Center for Computing Services:

1. Develop and implement standard configuration management policies and procedures for all CS sites.

Management Comments. The Director, CS, concurred and stated CS developed and implemented a standard configuration management plan effective as of December 2005.

2. Implement a standardized process to review, approve, and track configuration changes to systems. The process should include a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. The process should address the following:

a) Documented configuration change requests.

b) Configuration change specifications.

c) Test plans and results.

d) Written management approval.

e) Implementation schedule.

f) Documented customer acceptance, if applicable.

g) Documentation to reflect the change request closeout.

Management Comments. The Director, CS, concurred and stated CS implemented a standardized process to review, approve, and track configuration changes to systems. The process includes a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. These requirements are covered in the CS Operational Change and Configuration Management Plan, dated December 2005. In addition, test plans and results are done and documented for customers that have this requirement in their SLA.

3. Develop a process to ensure that binary or machine executable public domain software products, shareware and freeware are not installed on CS systems. This process should include regular inspections of workstations.

Management Comments. The Director, CS, concurred and stated CS has developed policy (CSD 06-03) to ensure that binary or machine executable public domain software products, shareware and freeware are not installed on CS systems. This process includes removing privileged user rights from workstations and monitoring through the implementation of an Administrative Local Area Network. Completion of this implementation is scheduled for September 2007.

4. Require personnel participation in configuration management functions to receive training in configuration management. Document the participation in training.

Management Comments. The Director, CS, concurred and stated CS is in the process of adapting Information Technology Infrastructure Library training for supervisors and Configuration Management Personnel. Training of current supervisors and Configuration Management Personnel is expected to be completed by September 2007. The documentation of the training will be tracked through the Defense Information Systems Agency On-Line Training System.

H. Enterprise Systems Management Application Controls

The general and application controls over the ESM applications were not fully effective. The controls were not effective because CS had not implemented adequate controls over the ESM applications. The ESM Program Management did not consistently develop, implement, and enforce effective system access controls. In addition, security documentation did not adequately address specific ESM application security requirements as required by DoD standards. Inadequate application security controls increase the risk of unauthorized disclosure of critical network management data; degrades availability or total loss of network management data and resources; and introduces unreliable network management data due to compromised data integrity.

Enterprise Systems Management Application

ESM addresses the challenges of managing the needs of heterogeneous computing environments by implementing processes, automation, and integration to improve and simplify IT management. The primary goal of the ESM applications is for CS to efficiently monitor and manage IT assets around the globe from a centralized location. DECC Montgomery is the primary production site mirrored by DECC Oklahoma City for disaster recovery. The ESM applications include the following:

- **Formula (Managed Objects)** provides the presentation layer through which the various levels of management, technicians, and customers view the environment. Events from each of the operating environments, including server and mainframe, were fed either through the Tivoli Enterprise Console or directly into the Formula server. HP OpenView feeds Managed Objects directly.

- **Trouble Management System (TMS**), a Remedy-based product, is used to create, assign, track, and resolve trouble tickets and to store, search for, and retrieve solutions to past problems.

- **HP OpenView Network** is a set of tools for network management, providing in-depth views of the network in a graphical format. These tools are used primarily by the CCCs to manage network devices and are accessed through Managed Objects.

- **Veritas Netbackup** delivers data protection when managing all aspects of backup and recovery. It allows consistent backup policies to be enforced across the enterprise. Veritas is an advanced media management tool with capabilities such as tape labeling; tape media pool creation, device sharing, media or device reporting, and bar code support.

CS had not implemented effective application controls over system access and security monitoring of the ESM applications: Formula (Managed Objects), HP OpenView, TMS, and Veritas Netbackup to ensure that only authorized users had access to these systems. Security documentation used to support security planning, policies, and procedures for the ESM applications did not adequately address specific ESM application security requirements. ESM applications must be able to perform two types of functions. First, they must handle functional domains such as account creation, security administration, system backups, configuration accounting, event monitoring, and more. Second, they must be able to share and correlate information and events across domains. Tests identified inadequate application controls and security documentation for the ESM applications.

Access Control

The ESM Program Management did not consistently develop, implement, and enforce effective system access controls, to include:

- account management,
- account logon,
- auditing and monitoring, and
- segregation of duties and controls to ensure the principle of least privilege.

Account Management. The controls over account management, to include creating, maintaining, and deleting individual accounts, were not adequately designed or operating effectively throughout the CS ESM application environment. Specifically, CS did not consistently require the use of a SAAR or equivalent, as required by the Handbook. The Handbook identifies these forms as the key control for managing access to all CS networks, systems, databases, and applications. In a sample we tested related to access to ESM systems, the three administrator accounts for HP OpenView had no exceptions. For the remaining three applications, 40 of the 133 SAARs were not provided, or were dated after the date of our initial request, as follows:

- Formula users – 14 of 45,
- TMS users – 25 of 45, and
- Veritas users – 1 of 43.

Of the remaining 93 forms, the majority contained one or more of the following errors.

- The form did not contain the system name or did not specify the application name for which access was requested.
- The justification for access was either incomplete or insufficient.

- The level of access required was not completed.
- The section to be filled in by the individual establishing the account was incomplete.
- The forms were completed after access had been granted.
- The same user has multiple forms requesting different access levels.
- The security manager verification had not been completed.

CS users had access to application systems that they no longer required for their job functions. DoD Instruction 8500.2 requires that system access only be granted to authorized personnel, and for the entity to develop procedures to ensure a periodic review of user lists for inactive accounts, validation of user access, timely notification of user terminations and transfers, and timely removal of user accounts. Without an effective process, CS is at increased risk that unauthorized personnel could access ESM applications and perform inappropriate and unauthorized procedures without being detected. In addition, without a formal process in place, CS cannot ensure that that only authorized users have been granted access to its systems, that an appropriate level of access is maintained for each user, and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated.

Account Logon. CS did not comply with DoD Instruction 8500.2 requirements that are specific to account logon for Formula, HP OpenView, and TMS applications, or with managing successive logons attempts. Specifically, each application allowed an unlimited number of invalid logon attempts without locking the account. In addition, HP OpenView logon sessions did not terminate after a specified period of inactivity and virtual private network users were allowed to remain logged on for 24 hours.

Formula and TMS application passwords did not meet DoD Instruction 8500.2 requirements for password length, complexity, history, and expiration requirements. For example, Formula had no minimum password length requirement; password composition that did not consist of at least one upper case, one lower case, alphanumeric, and special characters; passwords that did not expire; and unlimited invalid logon attempts. TMS had no minimum length requirement for passwords, no password composition requirements, no expiration period for passwords, and no limit on number of login attempts.

Without an effective account logon procedures, the risk is increased that unauthorized access could be made to CS systems without detection. Therefore, these applications would be vulnerable to password cracking or other attacks and exploitation that could be used to discover a user's password. As a result, a malicious user could acquire a user's password and gain unauthorized access to critical application functions and compromise the confidentiality, integrity, and availability of CS resources.

Auditing and Monitoring. The ESM applications did not consistently comply with DoD Instruction 8500.2, which requires the regular review of audit trails for inappropriate or unusual activity. For example, Veritas did not support audit logging, and no access monitoring capabilities existed for TMS. Formula administrators performed not only user account management, but also security-related functions. In addition, CS did not monitor ESM Central Application Administrators activities. For example, Veritas administrators circumvented application access controls by utilizing pseudo access to the root account. With the excess privileges, combined with the lack of a monitoring process, the ESM Central Application Administrators had the capability to perform unauthorized or inappropriate activities without being detected.

Segregation of Duties and Least Privilege. CS did not implement appropriate segregation of duties for privileged ESM users to comply with DoD Instruction 8500.2, which requires that access procedures enforce the principles of segregation of duties and least privilege. Specifically, CS did not implement appropriate segregation of duties within the ESM applications as follows:

- The Formula Central Application Administrator and Security Administrator functions were not separate and duties were performed by the same person;

- The HP OpenView administrator was granted root access to the UNIX server hosting HP OpenView; and

- At some locations, staff had overlapping responsibilities and Veritas users were also Security Administrators for Veritas.

The combination of inappropriate system access, which is incompatible with the application administrators' job responsibilities, and the lack of adequate monitoring of their systems activities increase the risk that unauthorized procedures could occur without being detected.

Documentation

Security documentation used to support security planning, policies, and procedures for the ESM applications did not adequately address specific ESM application security requirements as required by DoD standards. For example, the system security plan for Formula focused on requirements related to the UNIX and Windows NT operating systems, but did not provide enough detail to specifically address Formula's security requirements at the application layer. In addition, CS lacked specific ESM application STIGs or security recommendation guides; and lacked security documentation and procedures to supplement vendor technical manuals. DoD Instruction 8500.2 requires the development of a system security plan and regular review of that plan, as well as the use of a security configuration guide when deploying IT products. Without adequate policies and procedures and related documentation to support security planning, the risk is increased of weaknesses occurring in access controls and segregation of duties.

Recommendations and Management Comments

As a result of management comments, we redirected recommendation H.6.a.and H.6.c from the Director, CS to the Chief, FSO and renumbered recommendation H.6.a and H.6.c to H.7.a. and H.7.b.

H.1. We recommend that the Director, Center for Computing Services, develop a process to enforce the completion and maintenance of Systems Access Authorization Request forms or their equivalent to ensure consistency across all Enterprise Systems Management applications; and periodically review these forms for completeness and accuracy.

Management Comments. The Director, CS, concurred and stated CS implemented Privileged Attribute/Access Policy and Procedures (CSD 06-05) and the draft Security Handbook, released February 2006, that enforce the completion and maintenance of System Access Authorization Request or their equivalent to ensure consistency across all ESM applications and periodically review these forms for completeness and accuracy. The policy was effective as of November 2005.

H.2. We recommend that the Director, Center for Computing Services, monitor and periodic review of application administrator activities and application audit logs for inappropriate or unusual activity.

Management Comments. The Director, CS, concurred and stated CS will follow the minimal auditing requirement document developed in March 2006 by the FSO. This guidance will be followed until a standard set of auditing tools is provided by the FSO.

H.3. We recommend that the Director, Center for Computing Services, change the system settings to enforce:

a. An account lockout after a predefined number of invalid logon attempts.

Management Comments. The Director, CS, concurred and stated CS is in the process of updating all ESM applications to ensure they comply with account lockout settings, this will be accomplished for TMS by September 30, 2006, for Site Scope and TOPAZ[3] by October 31, 2006, and for Formula by November 30, 2006.

b. Session log offs after a predefined period of inactivity.

Management Comments. The Director, CS, concurred and stated CS is in the process of updating all ESM applications to ensure they comply with account session log offs after a predefined period of inactivity; this will be accomplished for KANA IQ, KANA Response and Crystal Reports[4] by September 30, 2006, for

[3] Site Scope and TOPAZ are other applications within the ESM Suite.

[4] KANA IQ, KANA Response and Crystal Reports are other applications within the ESM Suite.

Site Scope and TOPAZ by October 31, 2006, and for Formula by November 30, 2006.

c. Passwords compliance with current DoD Instruction 8500.2 requirements.

Management Comments. The Director, CS, concurred and stated CS is in the process of updating all ESM applications to ensure they comply with password compliance in accordance with DoD Instruction 8500.2, this will be accomplished for TMS by September 30, 2006, for Site Scope and TOPAZ by October 31, 2006, and for Formula by November 30, 2006.

H.4. We recommend that the Director, Center for Computing Services, enforce proper segregation of duties between application administrator, and application security administrator responsibilities.

Management Comments. The Director, CS, concurred and stated CS created a segregation of duties policy and procedure. CS implemented this policy effective March 15, 2006.

H.5. We recommend that the Director, Center for Computing Services, establish procedures to periodically recertify user access levels to ensure that access remains consistent with user job responsibilities.

Management Comments. The Director, CS, concurred and stated CS has established procedures to periodically recertify user access levels to ensure that access remains consistent with user job responsibilities in the draft Handbook issued in February 2006.

H.6. We recommend that the Director, Center for Computing Services, revise the Enterprise Systems Management Application system security plan to specifically address Enterprise Systems Management application information assurance requirements.

Management Comments. The Director, CS, concurred and stated CS will revise ESM tools IA requirements in accordance with Chief, FSO's recommendations. The security plan will be updated by December 31, 2006.

H.7. We recommend that the Chief, Field Security Operations, develop and implement comprehensive Enterprise Systems Management Application documentation, to include:

a. Developing specific information assurance requirements for Enterprise Systems Management Applications.

b. Develop specific Enterprise Systems Management application administrator technical implementation guides and procedures to supplement vendor technical manuals.

Management Comments. The Chief, FSO, concurred with both recommendations. The FSO has developed an ESM STIG. This STIG lays out the overall IA requirements for an ESM application. The ESM STIG also addresses the roles and responsibilities for the IA Office and system administrators and contains specific technical implementation guidance for Tivoli and Systems Management Service. The ESM STIG has been submitted to the Defense Information System Network Security Accreditation Working Group for review and signature. The current draft has been posted to the Information Assurance Support Environment web site for immediate reference.

Appendix A. Scope and Methodology

We performed an assessment of the design and operational effectiveness of the DISA CS controls at 16 data processing locations from October 1, 2004 through April 30, 2005. This assessment was performed in accordance with the American Institute of Certified Public Accountants Statement on Auditing Standards 70, as amended, and with generally accepted government auditing standards. We also assessed whether CS complied with applicable laws and regulations, including the Federal Financial Management Improvement Act and the FISMA. Additionally, we assessed whether CS properly certified and accredited its sites as required by the DITSCAP.

The audit methodology used to conduct the review was developed with the financial audit methodology established by the GAO Financial Audit Manual and FISCAM, including planning and internal controls, testing, and reporting phases. The FISCAM was the primary source document used to develop the detailed audit steps and to perform the review of the CS IT controls environment. The audit program was supplemented by the following DoD IA documentation: DoD Directive 8500.1, DoD Instruction 8500.2, DoD Instruction 5200.40, the Handbook, and DISA STIGs.

We interviewed key program personnel at selected CS site locations and tested general and application controls across CS, including CS Headquarters and DECCs.

General Controls. We conducted a full review of FISCAM controls at DECCs Columbus, Ohio; Mechanicsburg, Pennsylvania; Montgomery, Alabama; Ogden, Utah; Oklahoma City, Oklahoma; and St. Louis, Missouri. This review was based on the six key domains of FISCAM.

- **Entity-wide security program planning and management –** Risk assessment process, development and implementation of security program plans, personnel security, and audit follow-up.

- **Access controls –** Effectiveness of physical and logical access controls over IT assets.

- **Application software development and change control –** Controls over program changes.

- **System software** – Approved access to sensitive system utilities and tools, monitoring of use, and modifications of system software.

- **Segregation of duties –** Description of key functions and assignment of employee access and responsibilities using the concept of least privilege.

- **Service continuity –** Development and periodic updating and testing of contingency plans, and the establishment of environmental controls to minimize the potential loss of data due to a disaster.

We performed a limited FISCAM review over physical, environmental, and service continuity controls, at the remaining 10 DECC locations; Chambersburg, Pennsylvania; Dayton, Ohio; Denver, Colorado; Huntsville, Alabama; Jacksonville, Florida; Norfolk, Virginia; Rock Island, Illinois; San Antonio, Texas; San Diego, California; and Warner Robins, Georgia. The testing performed at these locations directly linked to FISCAM domains related to access controls and service continuity.

We reviewed the controls at CS Headquarters to obtain an understanding of the centralized functions of the organization. This included the establishment of entity-wide policies and procedures for risk assessment, security planning, and security management; personnel security and human resource management; SLAs; and compliance with government laws, including the Federal Financial Management Improvement Act, FISMA, and the Business Management Modernization Program.

The testing of the general controls environment also included system diagnostic testing and network penetration testing. The results of the diagnostic and penetration testing are outlined in separate technical reports and support the evaluation of general controls under the FISCAM methodology. They should be considered when concluding on the control design and effectiveness of the CS controls environment.

Application Controls. We reviewed application controls over the individual computerized applications owned and operated by CS. Specifically, we reviewed the ESM suite that CS uses to manage, operate, and secure the computing environment. We reviewed the following four ESM suite applications: Formula, TMS, HP OpenView Network, and Vertias Netbackup. The suite consists of processing systems located primarily at DECCs Montgomery and Oklahoma City. DECCs Columbus, Mechanicsburg, and Ogden have minimal ESM administrator responsibilities.

Sampling Methodology. We based our sampling on the GAO Financial Audit Manual, Section 450. When possible we selected judgmental samples of 45 at each site or used the entire population. Specifically, from lists of all active user accounts at the time of the site visits at DECCs Columbus, Mechanicsburg, Montgomery, Ogden, Oklahoma City, and St. Louis, we selected samples of 45 users for tests involving user access authorizations. Additionally, we reviewed and tested access removal policies and procedures for terminated employees at DECCs Columbus, Montgomery, Ogden, Oklahoma City, and St. Louis. We reviewed contingency plans, data backup and off-site storage, and safeguarding assets compliance at all 16 DECCs.

For the review of the four ESM suite applications, we requested the access control lists to obtain the user population at DECCs Columbus, Mechanicsburg, Montgomery, Ogden, and Oklahoma City. We judgmentally selected samples of 45 users for each of the four ESM suite applications, or used the entire user population for each application, to test account management of the ESM applications.

Finally, we used the samples pulled for the Unisys and UNIX devices from another report, Diagnostic Testing at the Defense Information Systems Agency Center for Computing Services, to support the configuration management and audit log setting findings from this report. The results of our review are not intended to be used to generalize that the general and application controls at CS sites were adequate or inadequate.

Use of Computer-Processed Data. We did not rely on computer-processed data to perform this audit. Rather, we assessed the general and application controls that involved computer-generated data such as user access listings and terminated employee listings.

Use of Technical Assistance. The Technical Assessment Division of the Office of Inspector General assisted in reviewing audit and test plans as well as testing compliance with DoD IA and certification and accreditation requirements. Additionally, we received assistance from the Quantitative Methods Division of the Office of Inspector General, to develop our sampling plan.

Government Accountability Office High-Risk Area. The GAO has identified several high-risk areas in DoD. This report provides coverage of the effective Management of Information Technology Investments high-risk area.

Prior Coverage

During the last five years, the GAO and DoD Office of Inspector General have issued three reports related to DISA CS systems security and general controls issues. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD Office of Inspector General reports can be accessed over the Internet at http://www.dodig.mil/audit/reports.

GAO

GAO Report No. GAO-02-50, "Defense Information Systems Agency Can Improve Investment Planning and Management Controls," March 2002

DoD IG

IG DoD Report No. D-2005-105, "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," September 6, 2005

IG DoD Report No. D-2002-148, "Defense Information Systems Agency Defense Enterprise Computing Center St. Louis Information Security Program," September 17, 2002

Appendix B. Compliance with Laws and Regulations

As part of the objective of the audit, we evaluated or attempted to evaluate compliance with the Federal Financial Management Improvement Act, FISMA, DITSCAP, and DoD Business Management Modernization Program.

Federal Financial Management Improvement Act

The Federal Financial Management Improvement Act of 1996 requires federal agencies to implement and maintain financial management systems that comply substantially with federal financial management systems requirements, applicable federal accounting standards, and the United States Government Standard General Ledger at the transaction level. The purpose of this law is to ensure that Federal financial management systems can provide consistent accounting of financial data to increase the productivity and transparency of federal financial management. The IG DoD has implemented a long-range strategy to audit the DoD information systems that provide supporting data to financial statements based on the Act.

This review was designed to use FISCAM to evaluate general computer controls over CS processing sites, which provide much of the processing support for DoD financial systems. Since CS primarily serves as a service provider for these systems, it does not manage the applications housed, which are generally managed and controlled by CS customers. Audit procedures related to the Act were not applicable for this review.

Federal Information Security Management Act

The Federal Information Security Management Act of 2002, Title III, requires each agency to develop, document, and implement an agency-wide information security program. The Act assigns agency heads, chief information officers, and inspectors general, responsibilities for information security, and implements requirements for annually reviewing agency information security programs. The annual review of the information security program includes the evaluation of the agency's system risk assessment, security awareness training, and implementation of a security plan, system incident response, and COOP for information systems. An annual independent evaluation of the information security program is performed and reported to OMB.

DoD is required to report compliance with the Act. DISA submits only one report addressing DISA as a whole. Because CS is just an organization within DISA, CS does not have its own FISMA report. FISMA requirements related to the CS system security program were integrated into our review of controls using the FISCAM methodology. The results and findings identified in this report may affect agency level FISMA reporting in the future.

DoD Information Technology Security Certification and Accreditation Process

The DoD Instruction 8500.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, directs a process for conducting uniform certifications and accreditations that support the agency's entity-wide security program. The DoD Manual 8510.1, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 31, 2000, was issued under the authority of DoD Instruction 5200.4, and is mandatory for use by all DoD components. The certification and accreditation process is designed to maintain the IA and security posture of DoD systems. System certification involves the comprehensive evaluation of the technical and non-technical security features and requirements using, for example, STIGs and Security Features User Guides. The certification process was designed to support the accreditation decision. System accreditation is the formal declaration by the Designated Approving Authority approving a system to operate in a particular security mode at an acceptable level of risk.

A System Security Authorization Agreement had been completed for each of the six DECCs where we performed our review procedures. Each DECC had received either a current Authority to Operate or an Interim Authority to Operate. Although the DITSCAP steps had been completed to receive an accreditation, at five sites weaknesses were identified, related to documentation support included in the System Security Authorization Agreement, and inconsistent system configurations identified during diagnostic testing. For example, DECC system security plans at DECCs Columbus, Montgomery, Ogden, Oklahoma City, and St. Louis were not consistently kept complete or current, and at DECC Ogden the Security Features User Guides were not developed for all technical platforms. The implementation of an effective DITSCAP process assists the Designated Approving Authority to make an informed accreditation decision, therefore reducing the risk that information systems without appropriate controls would be placed in production. Placing information systems into production without appropriate controls could increase the vulnerability of other trusted or connected systems, and negatively impact their confidentiality, integrity, and availability.

Business Management Modernization Program

DoD's Business Management Modernization Program Business Management Modernization Program was implemented to provide more efficient and effective means of using DoD system processing assets. The mission of BMMP is to transform business operations to achieve improved warfighter support while enabling financial accountability across the Department of Defense. The program is a large initiative and will require several years to complete. Based upon meetings with representatives for the DoD Enterprise Information Environment Mission Area and the Director of Business Modernization and System Integration during our review, program efforts were not at a stage where any meaningful testing could be performed. As a result, we subsequently removed this work from the scope of our review.

Appendix C. Transformation of the DECCs

In March 2003, CS officially announced its plans for transformation for its CONUS facilities. The CS transformation consists of four initiatives: (1) mainframe consolidation, (2) SMC consolidation, (3) Defense Finance and Accounting Service server consolidation, and (4) management restructuring. CS sites outside of CONUS were not included in the transformation.

The transformation will result in CS being highly centralized, highly standardized, secure, and efficient. Every aspect of CS' business and operations will focus on providing combat support computing to the warfighter. Operations will be centralized and consolidated in SMCs. In addition, business management, resource management, engineering, acquisition, logistics, workforce management, administration, and other overhead functions will be integrated and consolidated into a single virtual management organization.

Prior to the transformation, DISA computing centers were called DECCs and subordinate activities were called DECC Detachments. DECCs and DECC Detachments were part of the CS, which was previously called Computing Services Directorate and DISA Western Hemisphere. Under the transformation initiative, all computing sites will be called DECCs but will have functional designations, including SMCs, ISCs, and PEs.

Pre-Transformation Designation	**Post-Transformation Designation**
DECC Columbus, OH	ISC Columbus, OH
DECC Detachment Denver, CO	PE Denver, CO
DECC Detachment Indianapolis, IN	Decommissioned
DECC Mechanicsburg, PA	SMC Mechanicsburg, PA
DECC Detachment Chambersburg, PA	PE Chambersburg, PA
DECC Detachment San Diego, CA	PE San Diego, CA
DECC Detachment Norfolk, VA	PE Norfolk, VA
DECC Detachment Jacksonville, FL	PE Jacksonville, FL
CS Point of Presence Puget Sound, WA	CS Point of Presence Puget Sound, WA
DECC Ogden, UT	SMC Ogden, UT
DECC Detachment Dayton, OH	PE Dayton, OH
DECC Oklahoma City, OK	SMC Oklahoma City, OK
DECC Detachment Montgomery, AL	SMC Montgomery, AL
DECC Detachment Warner Robins, GA	PE Warner Robins, GA
DECC Detachment San Antonio, TX	ISC San Antonio, TX
DECC St. Louis, MO	PE St. Louis, MO
DECC Detachment Huntsville, AL	PE Huntsville, AL
DECC Detachment Rock Island, IL	PE Rock Island, IL

The technical support and help desk functions were performed at all processing sites prior to the transformation. When the transformation is complete, CS would have consolidated systems management and customer support functions for the mainframe and server computing environments into four SMC locations. There would be 12 PEs that maintain systems that are remotely managed by the SMC.

System Management Centers. Each SMC will consist of customer-focused Operations Support Teams and a Technical Support Section. The Operations Support Teams will provide all the service and knowledge elements that pertain to a customer's post deployment support. These services include the traditional Tier 1 help desk support, traditional basic console and operations support for the customer's applications, basic system monitoring for the customer's platforms and applications, and key skills required to be responsive to that customer. The Operations Support Teams have access to the Technical Support Sections within the SMCs that provide high level expertise for the installation, configuration, operations, and maintenance of platforms, databases, networks, and other enterprise functions. If necessary, these Technical Support Sections provide diagnostic support and fix actions for referred tickets that cannot be handled by the Operations Support Teams. The Technical Support Sections also update the common knowledge base to provide agents with the best solutions for known problems. Both elements of the customer support cycle are accountable to the same SMC management chain.

Infrastructure Service Centers. The ISC will perform system management for specialized fielding efforts from CS customers.

Processing Elements. The PEs will be staffed as "lights-dim" operations The PEs have a limited staff to perform touch labor, including device, component, and cable movement, installation, resetting, and hands-on console operations as required by the SMC or CCC and site security and facility management. PEs assist the SMC and CCC as required.

CS has established two CCCs to provide centralized network management for all 18 DECC locations to maintain a secure, cost effective, efficient, and reliable telecommunications operations environment supporting DoD and the warfighter. Utilizing a secure "out of band" management network, the CCCs support all routing, switching, domain name servers, and wide area network connectivity to DISA Network Services, and network security device operations. The CCCs also employ a Security Management Team to maintain the security functions on their production networks, including access control and intrusion detection services, firewall operations, and configuration management.

Prior to the transformation the DECCs managed their own budgeting, resource management, manpower, personnel, training, business proposals, and SLAs. With the transformation, these functions are being consolidated into three primary Business Support Management Centers: CS Headquarters, the Blue Ridge Center located in Chambersburg, and the Rocky Mountain Center located in Denver.

Appendix D. Acronyms

CCB	Change Control Board
CCC	Communications Control Centers
CM	Configuration Management
CONUS	Continental United States
COOP	Continuity of Operations Plan
CS	Center for Computing Services
DECC	Defense Enterprise Computing Center
DISA	Defense Information Systems Agency
DITSCAP	Department of Defense Information Technology Security Certifications and Accreditation Process
ESM	Enterprise Systems Management
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FSO	Field Security Operations
GAO	Government Accountability Office
IA	Information Assurance
IAM	Information Assurance Manager
ISC	Infrastructure Services Center
IT	Information Technology
MAC	Mission Assurance Category
OMB	Office of Management and Budget
PE	Processing Element
SAAR	System Access Authorization Request
SLA	Service Level Agreement
SMC	System Management Center
SSO	Systems Support Office
STIG	Security Technical Implementation Guide
TMS	Trouble Management System

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)/Chief Financial Officer
Deputy Chief Financial Officer

Combatant Commands

Commander, U.S. Strategic Command

Other Defense Organizations

Director, Defense Information Systems Agency

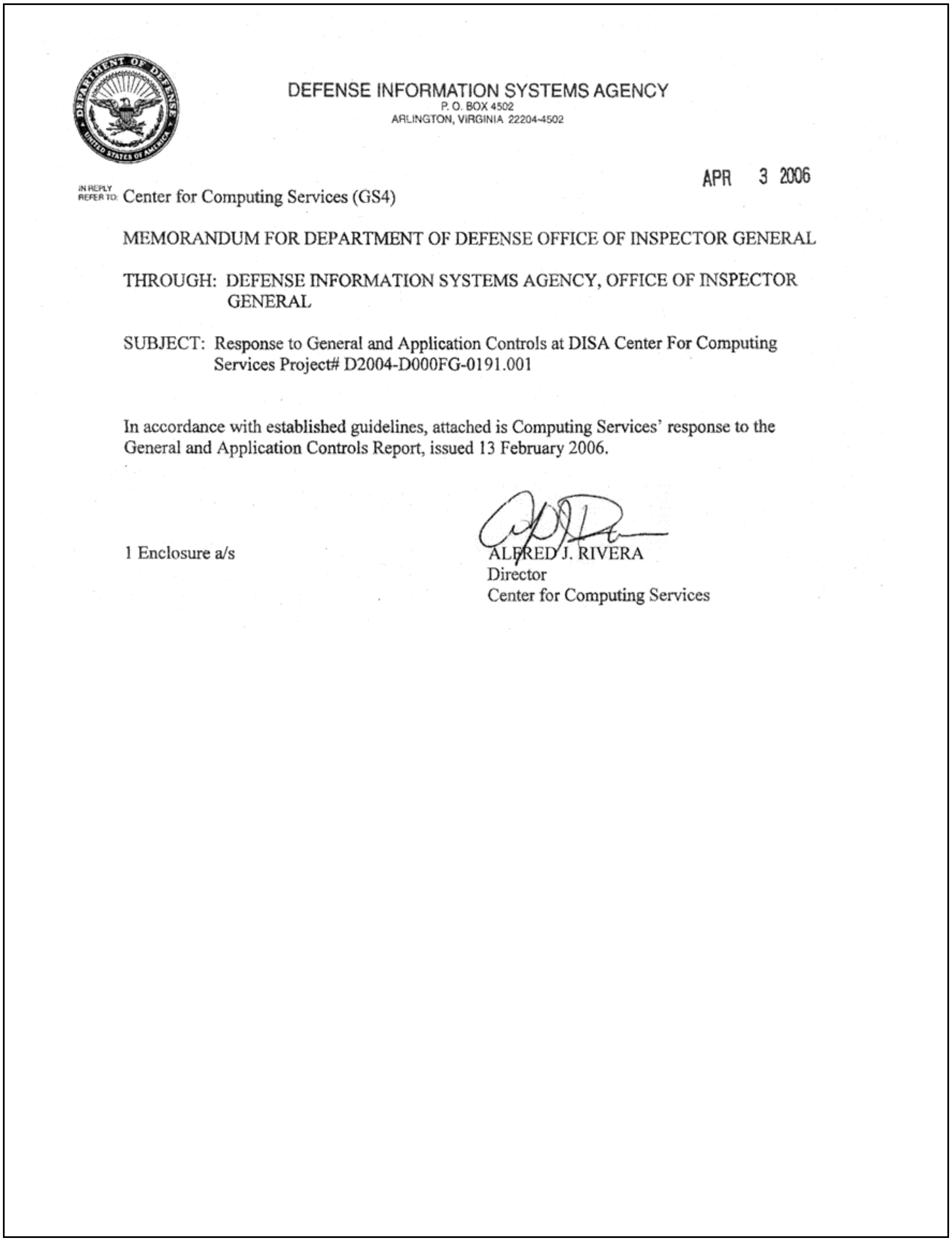
Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management and Accountability
House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Defense Information Systems Agency, Center for Computing Services Comments



DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 4502
ARLINGTON, VIRGINIA 22204-4502

APR 3 2006

IN REPLY REFER TO: Center for Computing Services (GS4)

MEMORANDUM FOR DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

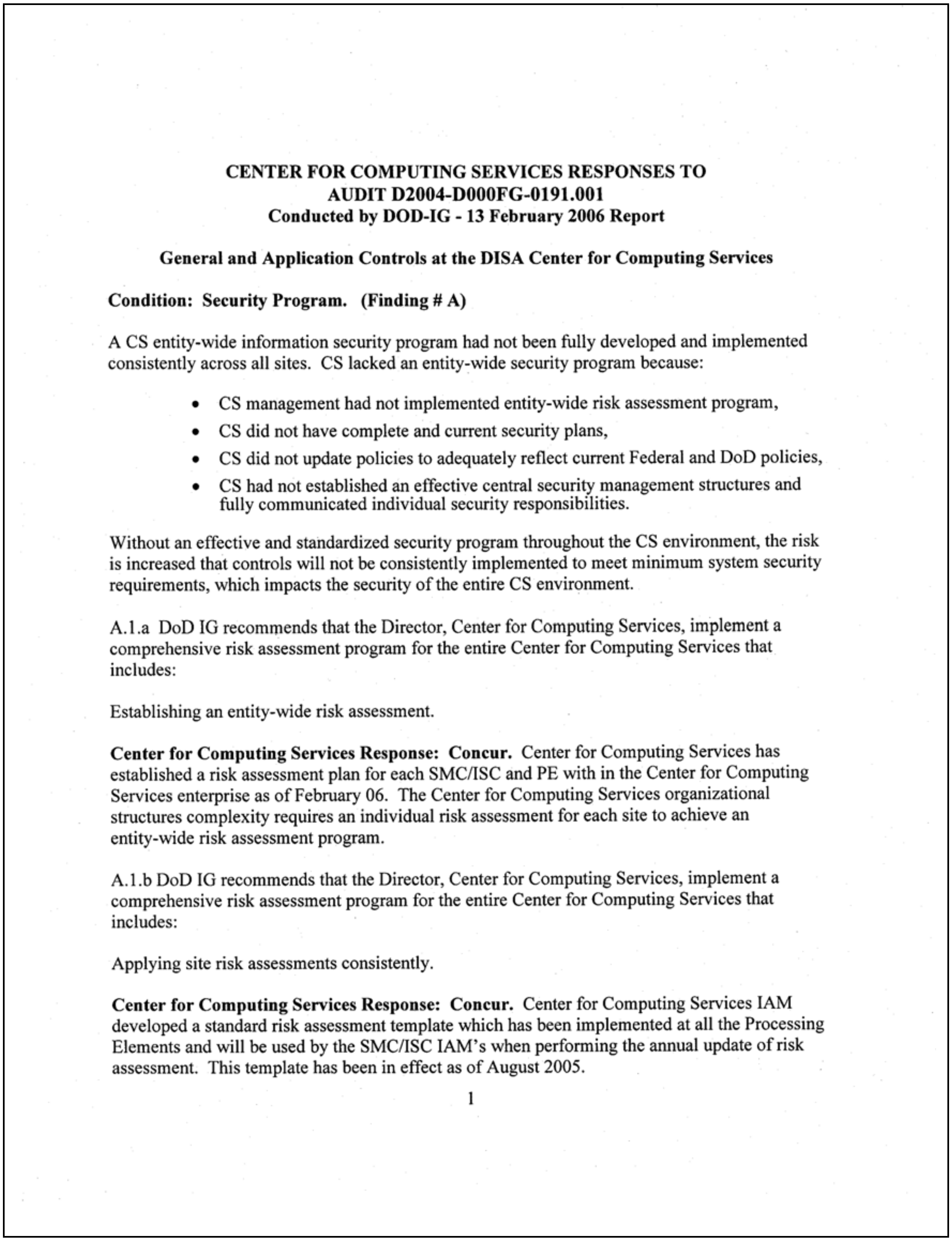
THROUGH: DEFENSE INFORMATION SYSTEMS AGENCY, OFFICE OF INSPECTOR GENERAL

SUBJECT: Response to General and Application Controls at DISA Center For Computing Services Project# D2004-D000FG-0191.001

In accordance with established guidelines, attached is Computing Services' response to the General and Application Controls Report, issued 13 February 2006.

1 Enclosure a/s

ALFRED J. RIVERA
Director
Center for Computing Services



CENTER FOR COMPUTING SERVICES RESPONSES TO
AUDIT D2004-D000FG-0191.001
Conducted by DOD-IG - 13 February 2006 Report

General and Application Controls at the DISA Center for Computing Services

Condition: Security Program. (Finding # A)

A CS entity-wide information security program had not been fully developed and implemented consistently across all sites. CS lacked an entity-wide security program because:

- CS management had not implemented entity-wide risk assessment program,
- CS did not have complete and current security plans,
- CS did not update policies to adequately reflect current Federal and DoD policies,
- CS had not established an effective central security management structures and fully communicated individual security responsibilities.

Without an effective and standardized security program throughout the CS environment, the risk is increased that controls will not be consistently implemented to meet minimum system security requirements, which impacts the security of the entire CS environment.

A.1.a DoD IG recommends that the Director, Center for Computing Services, implement a comprehensive risk assessment program for the entire Center for Computing Services that includes:

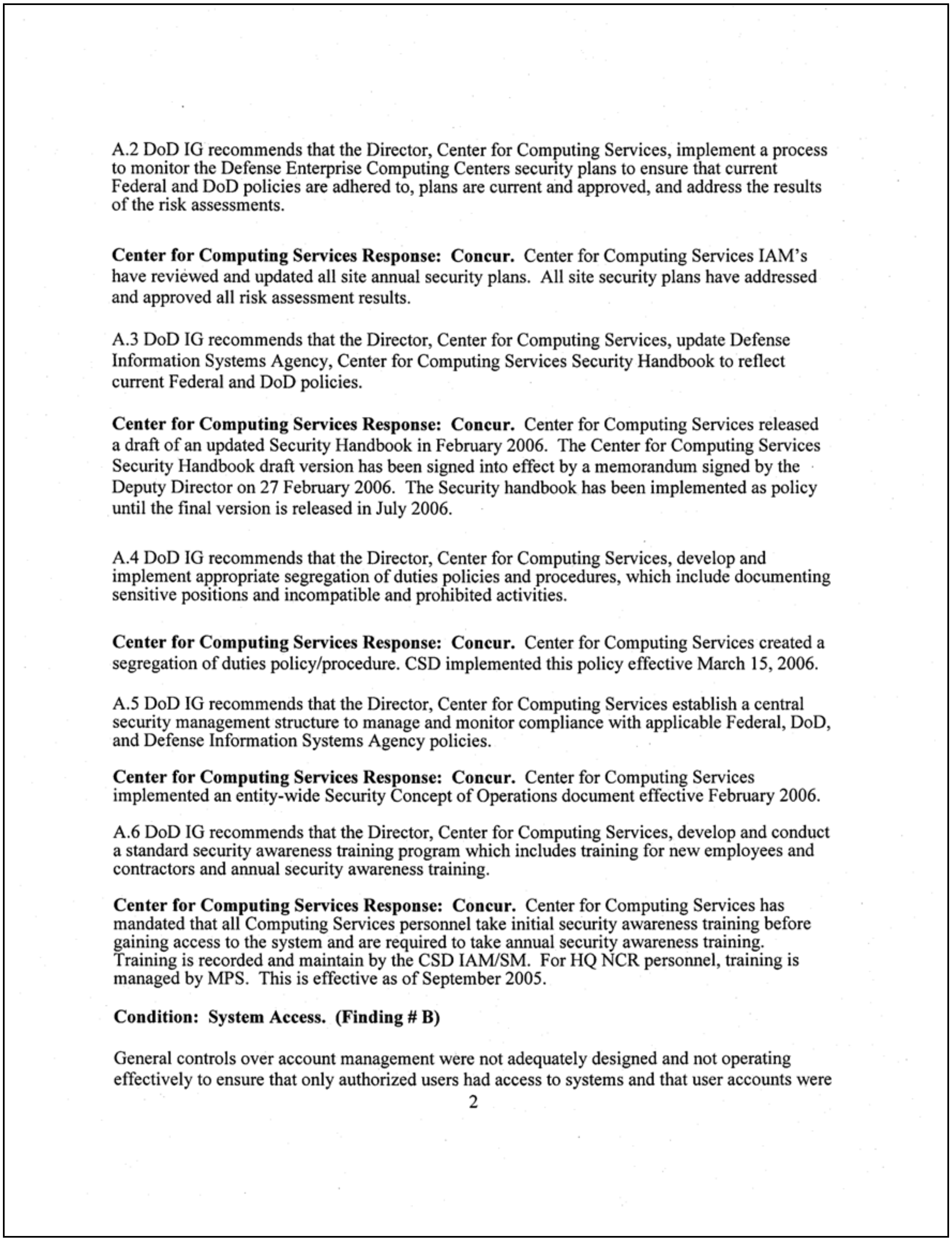
Establishing an entity-wide risk assessment.

Center for Computing Services Response: Concur. Center for Computing Services has established a risk assessment plan for each SMC/ISC and PE with in the Center for Computing Services enterprise as of February 06. The Center for Computing Services organizational structures complexity requires an individual risk assessment for each site to achieve an entity-wide risk assessment program.

A.1.b DoD IG recommends that the Director, Center for Computing Services, implement a comprehensive risk assessment program for the entire Center for Computing Services that includes:

Applying site risk assessments consistently.

Center for Computing Services Response: Concur. Center for Computing Services IAM developed a standard risk assessment template which has been implemented at all the Processing Elements and will be used by the SMC/ISC IAM's when performing the annual update of risk assessment. This template has been in effect as of August 2005.



A.2 DoD IG recommends that the Director, Center for Computing Services, implement a process to monitor the Defense Enterprise Computing Centers security plans to ensure that current Federal and DoD policies are adhered to, plans are current and approved, and address the results of the risk assessments.

Center for Computing Services Response: Concur. Center for Computing Services IAM's have reviewed and updated all site annual security plans. All site security plans have addressed and approved all risk assessment results.

A.3 DoD IG recommends that the Director, Center for Computing Services, update Defense Information Systems Agency, Center for Computing Services Security Handbook to reflect current Federal and DoD policies.

Center for Computing Services Response: Concur. Center for Computing Services released a draft of an updated Security Handbook in February 2006. The Center for Computing Services Security Handbook draft version has been signed into effect by a memorandum signed by the Deputy Director on 27 February 2006. The Security handbook has been implemented as policy until the final version is released in July 2006.

A.4 DoD IG recommends that the Director, Center for Computing Services, develop and implement appropriate segregation of duties policies and procedures, which include documenting sensitive positions and incompatible and prohibited activities.

Center for Computing Services Response: Concur. Center for Computing Services created a segregation of duties policy/procedure. CSD implemented this policy effective March 15, 2006.

A.5 DoD IG recommends that the Director, Center for Computing Services establish a central security management structure to manage and monitor compliance with applicable Federal, DoD, and Defense Information Systems Agency policies.

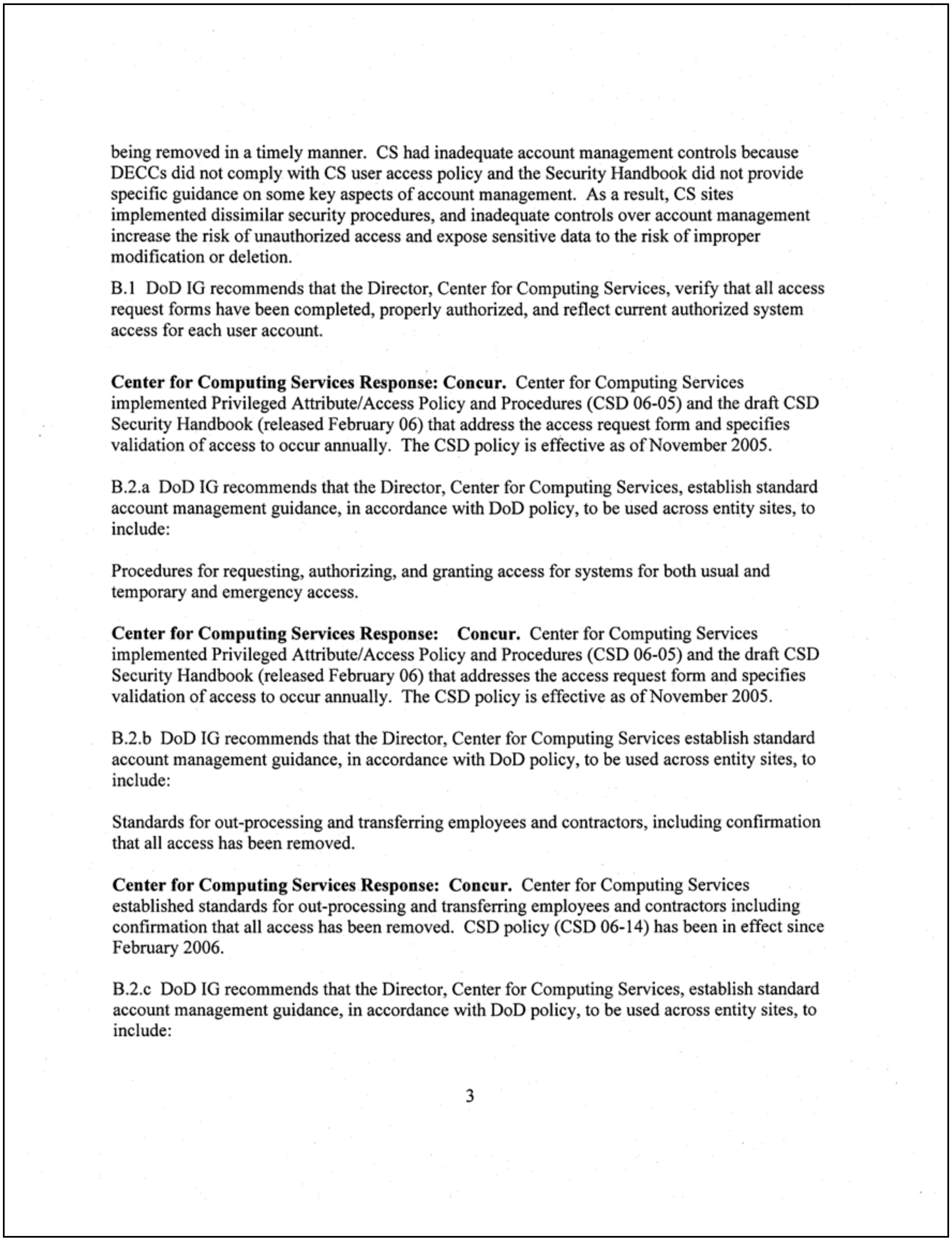
Center for Computing Services Response: Concur. Center for Computing Services implemented an entity-wide Security Concept of Operations document effective February 2006.

A.6 DoD IG recommends that the Director, Center for Computing Services, develop and conduct a standard security awareness training program which includes training for new employees and contractors and annual security awareness training.

Center for Computing Services Response: Concur. Center for Computing Services has mandated that all Computing Services personnel take initial security awareness training before gaining access to the system and are required to take annual security awareness training. Training is recorded and maintain by the CSD IAM/SM. For HQ NCR personnel, training is managed by MPS. This is effective as of September 2005.

Condition: System Access. (Finding # B)

General controls over account management were not adequately designed and not operating effectively to ensure that only authorized users had access to systems and that user accounts were



being removed in a timely manner. CS had inadequate account management controls because DECCs did not comply with CS user access policy and the Security Handbook did not provide specific guidance on some key aspects of account management. As a result, CS sites implemented dissimilar security procedures, and inadequate controls over account management increase the risk of unauthorized access and expose sensitive data to the risk of improper modification or deletion.

B.1 DoD IG recommends that the Director, Center for Computing Services, verify that all access request forms have been completed, properly authorized, and reflect current authorized system access for each user account.

Center for Computing Services Response: Concur. Center for Computing Services implemented Privileged Attribute/Access Policy and Procedures (CSD 06-05) and the draft CSD Security Handbook (released February 06) that address the access request form and specifies validation of access to occur annually. The CSD policy is effective as of November 2005.

B.2.a DoD IG recommends that the Director, Center for Computing Services, establish standard account management guidance, in accordance with DoD policy, to be used across entity sites, to include:

Procedures for requesting, authorizing, and granting access for systems for both usual and temporary and emergency access.

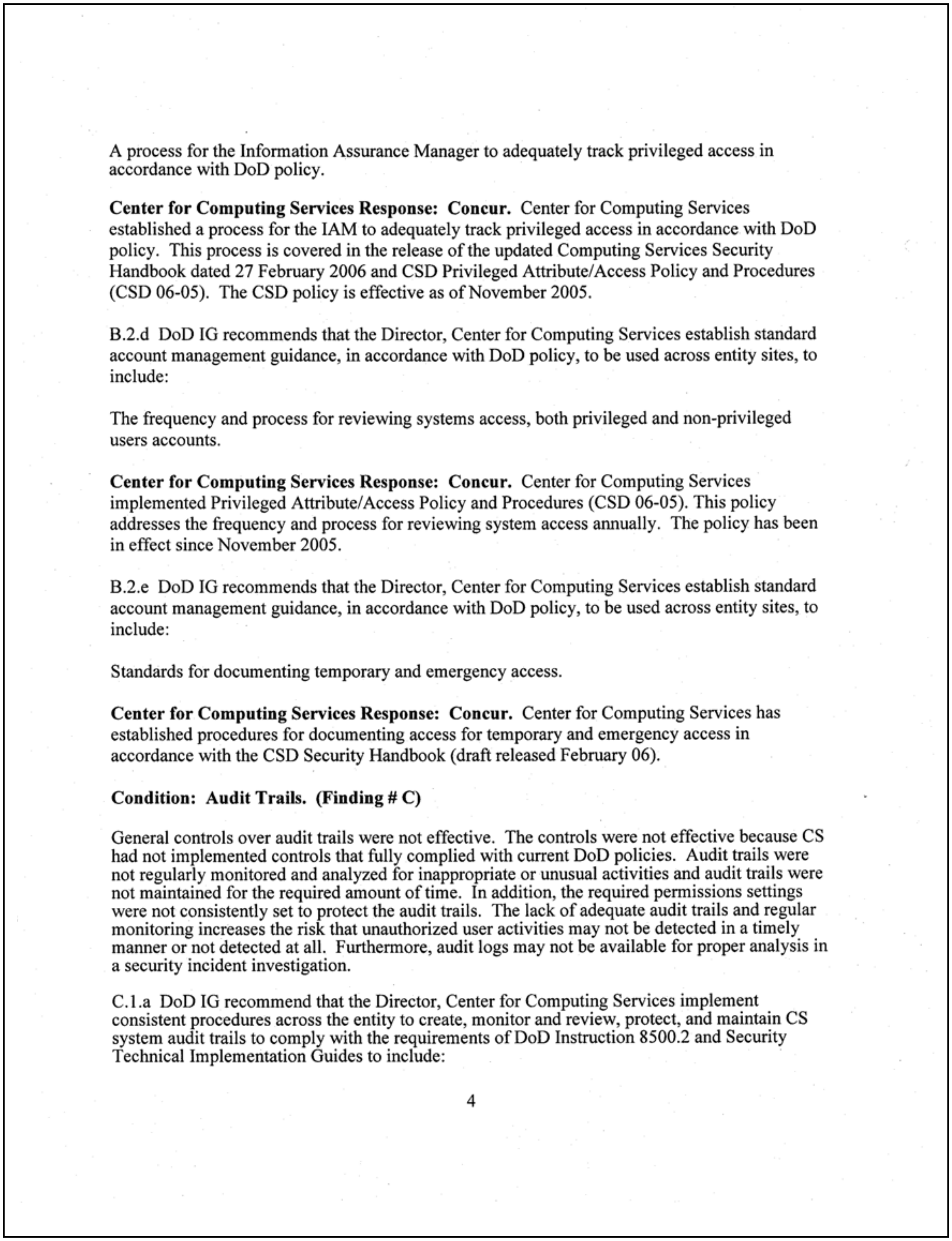
Center for Computing Services Response: Concur. Center for Computing Services implemented Privileged Attribute/Access Policy and Procedures (CSD 06-05) and the draft CSD Security Handbook (released February 06) that addresses the access request form and specifies validation of access to occur annually. The CSD policy is effective as of November 2005.

B.2.b DoD IG recommends that the Director, Center for Computing Services establish standard account management guidance, in accordance with DoD policy, to be used across entity sites, to include:

Standards for out-processing and transferring employees and contractors, including confirmation that all access has been removed.

Center for Computing Services Response: Concur. Center for Computing Services established standards for out-processing and transferring employees and contractors including confirmation that all access has been removed. CSD policy (CSD 06-14) has been in effect since February 2006.

B.2.c DoD IG recommends that the Director, Center for Computing Services, establish standard account management guidance, in accordance with DoD policy, to be used across entity sites, to include:



A process for the Information Assurance Manager to adequately track privileged access in accordance with DoD policy.

Center for Computing Services Response: Concur. Center for Computing Services established a process for the IAM to adequately track privileged access in accordance with DoD policy. This process is covered in the release of the updated Computing Services Security Handbook dated 27 February 2006 and CSD Privileged Attribute/Access Policy and Procedures (CSD 06-05). The CSD policy is effective as of November 2005.

B.2.d DoD IG recommends that the Director, Center for Computing Services establish standard account management guidance, in accordance with DoD policy, to be used across entity sites, to include:

The frequency and process for reviewing systems access, both privileged and non-privileged users accounts.

Center for Computing Services Response: Concur. Center for Computing Services implemented Privileged Attribute/Access Policy and Procedures (CSD 06-05). This policy addresses the frequency and process for reviewing system access annually. The policy has been in effect since November 2005.

B.2.e DoD IG recommends that the Director, Center for Computing Services establish standard account management guidance, in accordance with DoD policy, to be used across entity sites, to include:

Standards for documenting temporary and emergency access.

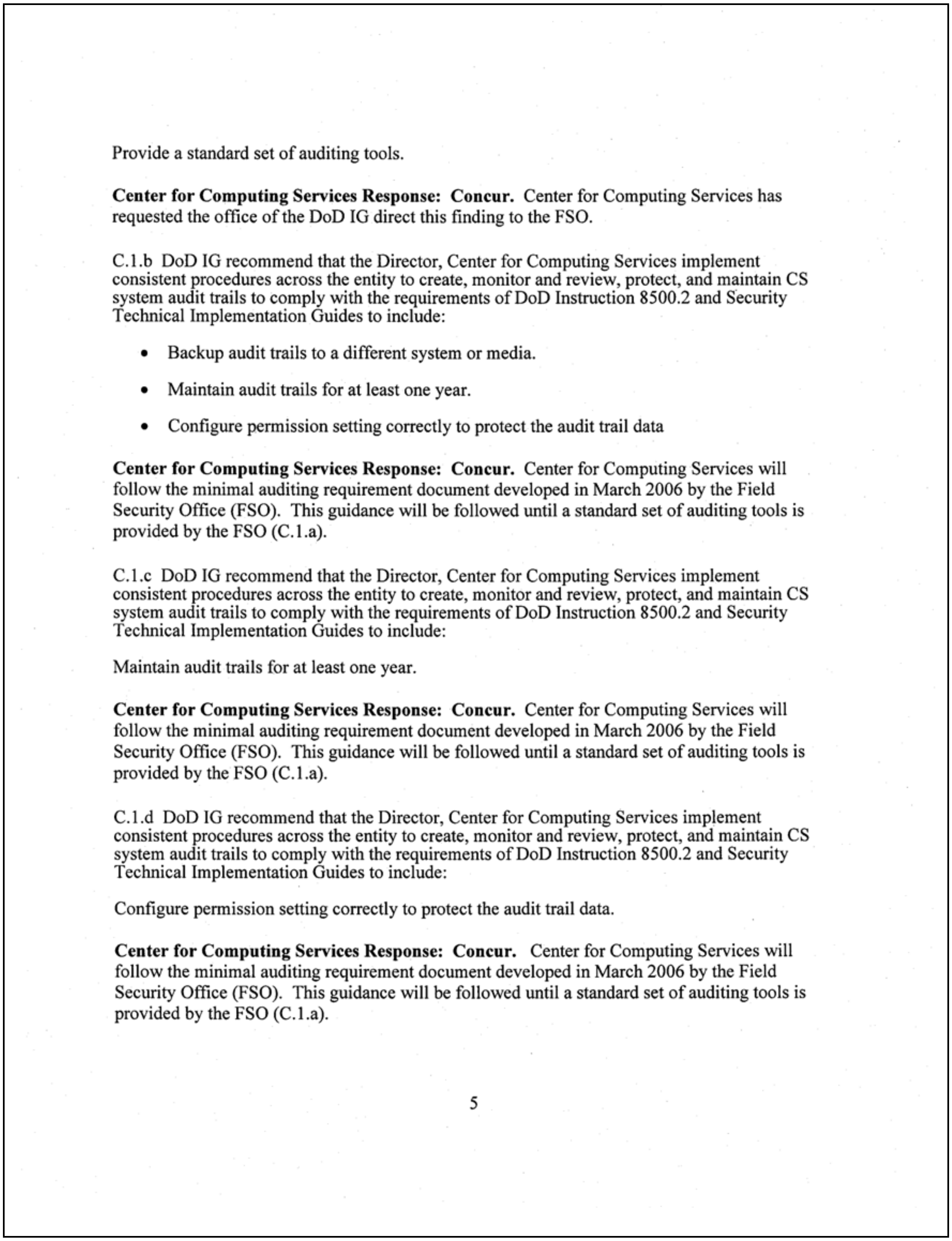
Center for Computing Services Response: Concur. Center for Computing Services has established procedures for documenting access for temporary and emergency access in accordance with the CSD Security Handbook (draft released February 06).

Condition: Audit Trails. (Finding # C)

General controls over audit trails were not effective. The controls were not effective because CS had not implemented controls that fully complied with current DoD policies. Audit trails were not regularly monitored and analyzed for inappropriate or unusual activities and audit trails were not maintained for the required amount of time. In addition, the required permissions settings were not consistently set to protect the audit trails. The lack of adequate audit trails and regular monitoring increases the risk that unauthorized user activities may not be detected in a timely manner or not detected at all. Furthermore, audit logs may not be available for proper analysis in a security incident investigation.

C.1.a DoD IG recommend that the Director, Center for Computing Services implement consistent procedures across the entity to create, monitor and review, protect, and maintain CS system audit trails to comply with the requirements of DoD Instruction 8500.2 and Security Technical Implementation Guides to include:

Final Report
Reference



Provide a standard set of auditing tools.

C2 **Center for Computing Services Response: Concur.** Center for Computing Services has requested the office of the DoD IG direct this finding to the FSO.

C.1.a C.1.b DoD IG recommend that the Director, Center for Computing Services implement consistent procedures across the entity to create, monitor and review, protect, and maintain CS system audit trails to comply with the requirements of DoD Instruction 8500.2 and Security Technical Implementation Guides to include:

- Backup audit trails to a different system or media.
- Maintain audit trails for at least one year.
- Configure permission setting correctly to protect the audit trail data

Center for Computing Services Response: Concur. Center for Computing Services will follow the minimal auditing requirement document developed in March 2006 by the Field Security Office (FSO). This guidance will be followed until a standard set of auditing tools is provided by the FSO (C.1.a).

C.1.b C.1.c DoD IG recommend that the Director, Center for Computing Services implement consistent procedures across the entity to create, monitor and review, protect, and maintain CS system audit trails to comply with the requirements of DoD Instruction 8500.2 and Security Technical Implementation Guides to include:

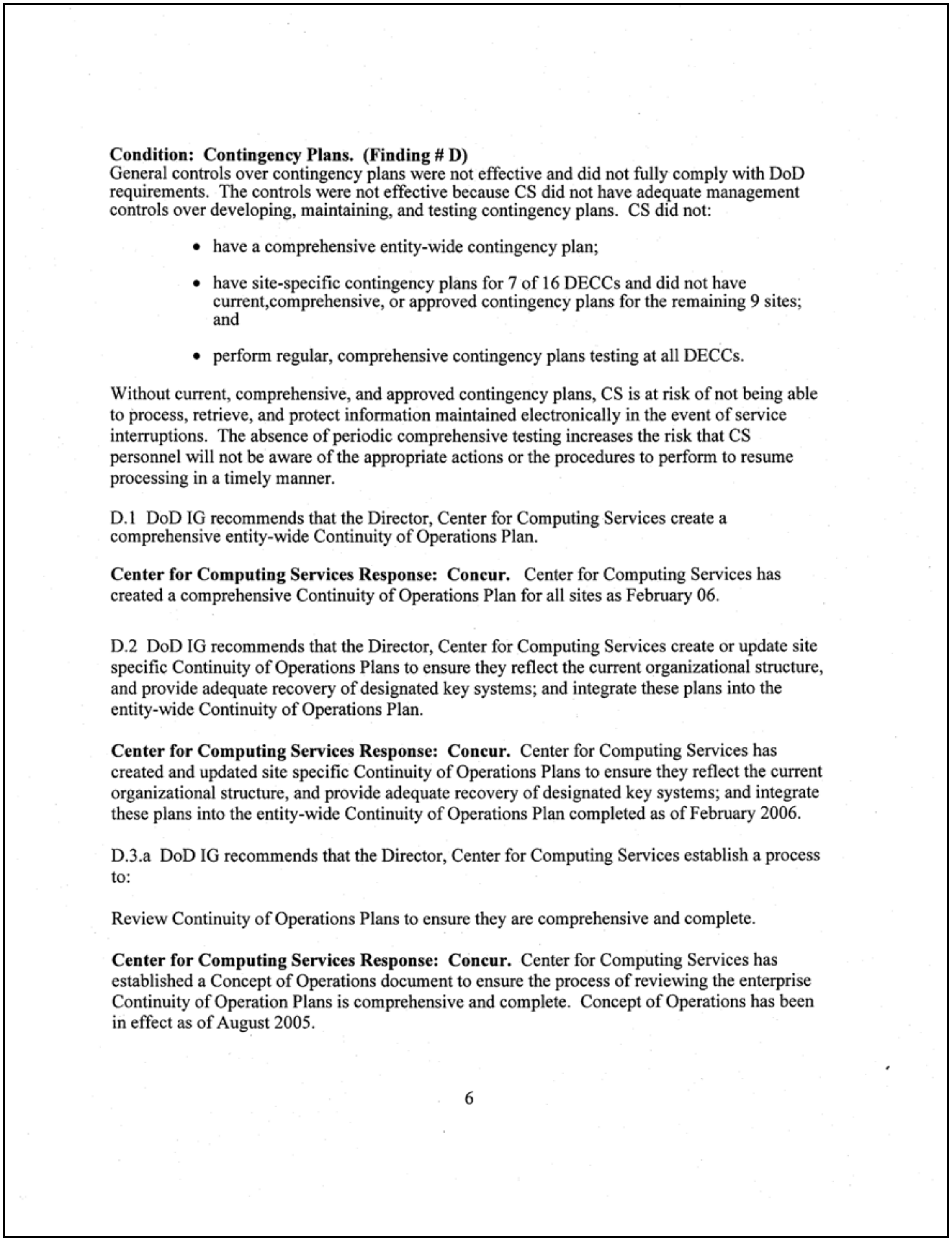
Maintain audit trails for at least one year.

Center for Computing Services Response: Concur. Center for Computing Services will follow the minimal auditing requirement document developed in March 2006 by the Field Security Office (FSO). This guidance will be followed until a standard set of auditing tools is provided by the FSO (C.1.a).

C.1.c C.1.d DoD IG recommend that the Director, Center for Computing Services implement consistent procedures across the entity to create, monitor and review, protect, and maintain CS system audit trails to comply with the requirements of DoD Instruction 8500.2 and Security Technical Implementation Guides to include:

Configure permission setting correctly to protect the audit trail data.

Center for Computing Services Response: Concur. Center for Computing Services will follow the minimal auditing requirement document developed in March 2006 by the Field Security Office (FSO). This guidance will be followed until a standard set of auditing tools is provided by the FSO (C.1.a).



Condition: Contingency Plans. (Finding # D)
General controls over contingency plans were not effective and did not fully comply with DoD requirements. The controls were not effective because CS did not have adequate management controls over developing, maintaining, and testing contingency plans. CS did not:

- have a comprehensive entity-wide contingency plan;
- have site-specific contingency plans for 7 of 16 DECCs and did not have current,comprehensive, or approved contingency plans for the remaining 9 sites; and
- perform regular, comprehensive contingency plans testing at all DECCs.

Without current, comprehensive, and approved contingency plans, CS is at risk of not being able to process, retrieve, and protect information maintained electronically in the event of service interruptions. The absence of periodic comprehensive testing increases the risk that CS personnel will not be aware of the appropriate actions or the procedures to perform to resume processing in a timely manner.

D.1 DoD IG recommends that the Director, Center for Computing Services create a comprehensive entity-wide Continuity of Operations Plan.

Center for Computing Services Response: Concur. Center for Computing Services has created a comprehensive Continuity of Operations Plan for all sites as February 06.

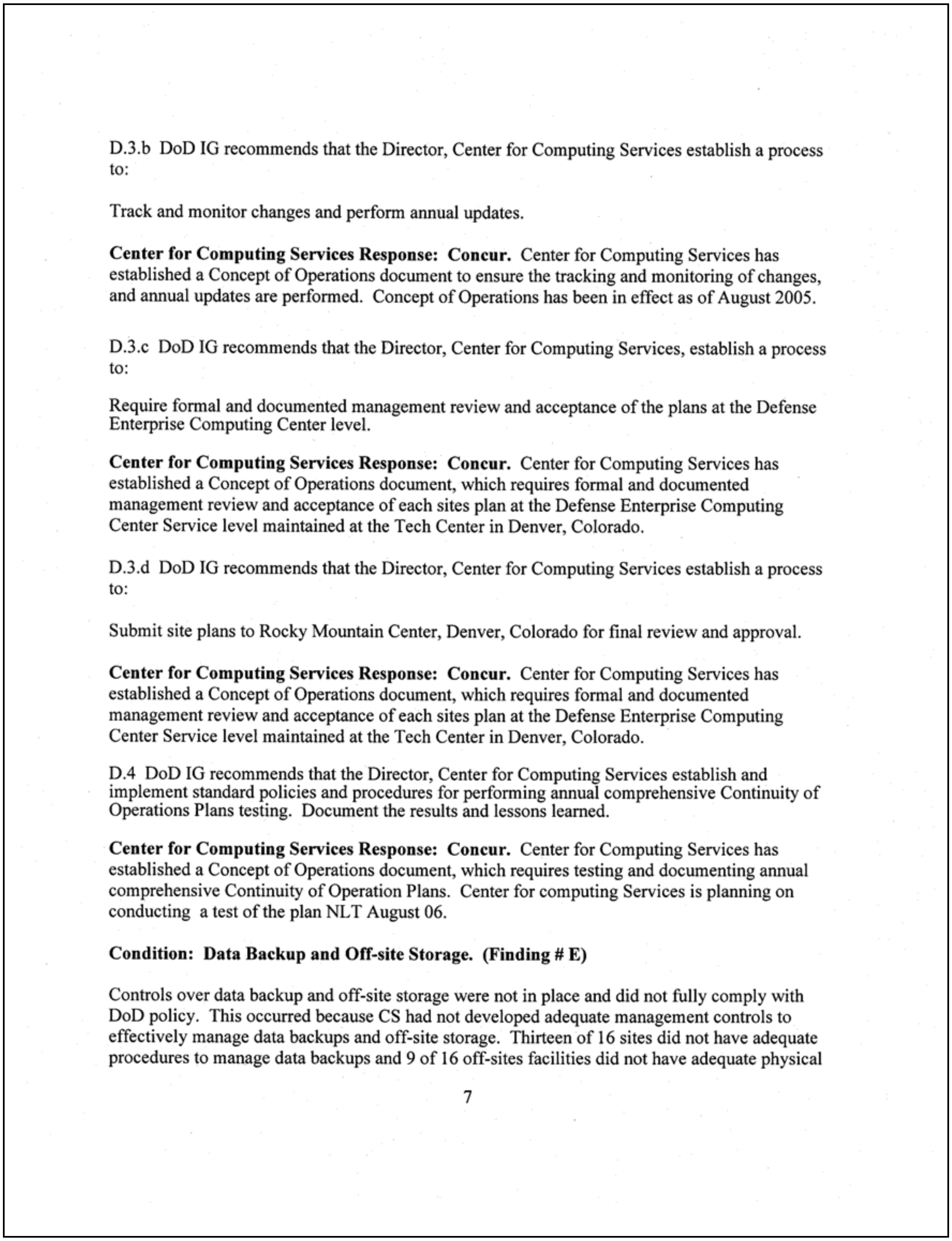
D.2 DoD IG recommends that the Director, Center for Computing Services create or update site specific Continuity of Operations Plans to ensure they reflect the current organizational structure, and provide adequate recovery of designated key systems; and integrate these plans into the entity-wide Continuity of Operations Plan.

Center for Computing Services Response: Concur. Center for Computing Services has created and updated site specific Continuity of Operations Plans to ensure they reflect the current organizational structure, and provide adequate recovery of designated key systems; and integrate these plans into the entity-wide Continuity of Operations Plan completed as of February 2006.

D.3.a DoD IG recommends that the Director, Center for Computing Services establish a process to:

Review Continuity of Operations Plans to ensure they are comprehensive and complete.

Center for Computing Services Response: Concur. Center for Computing Services has established a Concept of Operations document to ensure the process of reviewing the enterprise Continuity of Operation Plans is comprehensive and complete. Concept of Operations has been in effect as of August 2005.



D.3.b DoD IG recommends that the Director, Center for Computing Services establish a process to:

Track and monitor changes and perform annual updates.

Center for Computing Services Response: Concur. Center for Computing Services has established a Concept of Operations document to ensure the tracking and monitoring of changes, and annual updates are performed. Concept of Operations has been in effect as of August 2005.

D.3.c DoD IG recommends that the Director, Center for Computing Services, establish a process to:

Require formal and documented management review and acceptance of the plans at the Defense Enterprise Computing Center level.

Center for Computing Services Response: Concur. Center for Computing Services has established a Concept of Operations document, which requires formal and documented management review and acceptance of each sites plan at the Defense Enterprise Computing Center Service level maintained at the Tech Center in Denver, Colorado.

D.3.d DoD IG recommends that the Director, Center for Computing Services establish a process to:

Submit site plans to Rocky Mountain Center, Denver, Colorado for final review and approval.

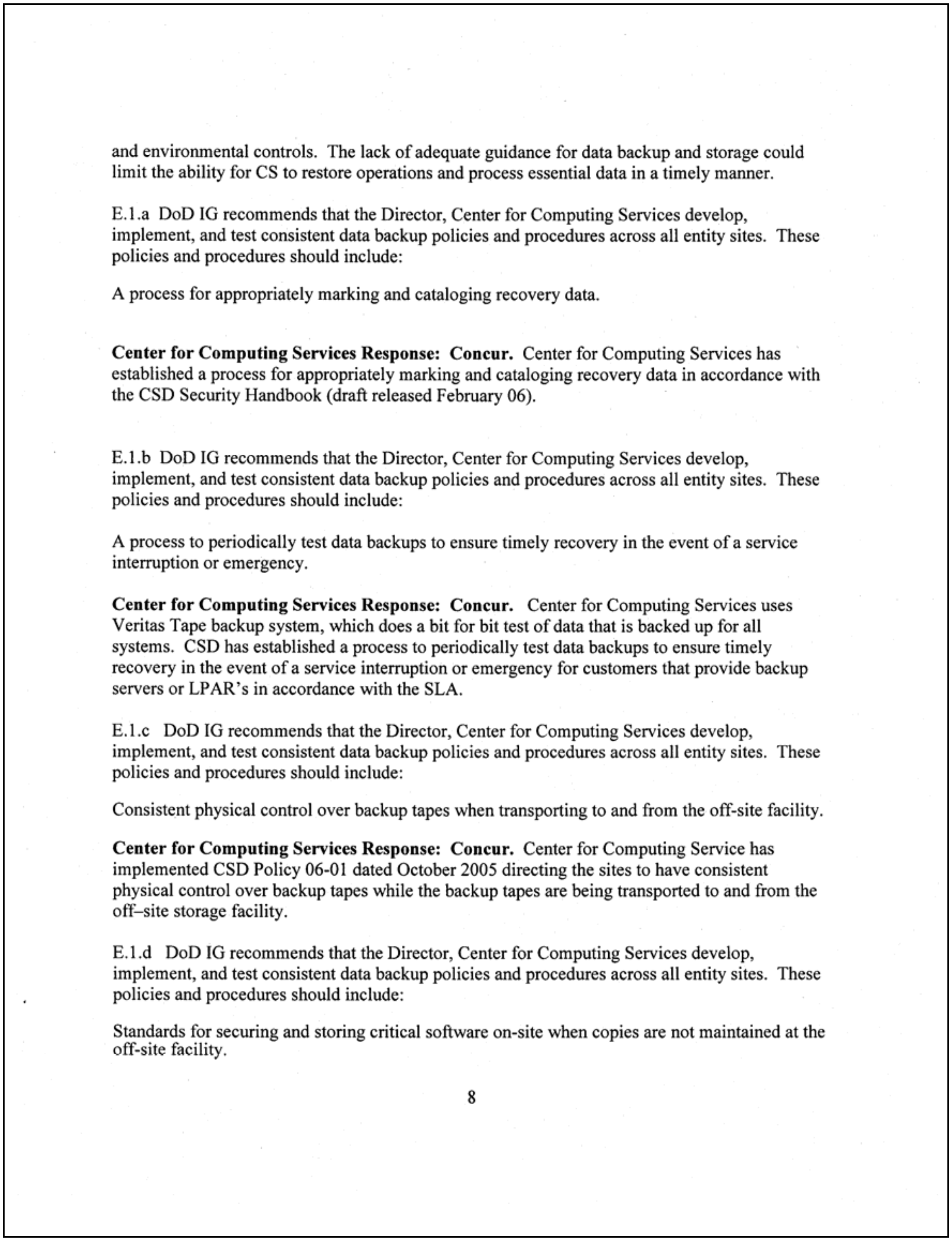
Center for Computing Services Response: Concur. Center for Computing Services has established a Concept of Operations document, which requires formal and documented management review and acceptance of each sites plan at the Defense Enterprise Computing Center Service level maintained at the Tech Center in Denver, Colorado.

D.4 DoD IG recommends that the Director, Center for Computing Services establish and implement standard policies and procedures for performing annual comprehensive Continuity of Operations Plans testing. Document the results and lessons learned.

Center for Computing Services Response: Concur. Center for Computing Services has established a Concept of Operations document, which requires testing and documenting annual comprehensive Continuity of Operation Plans. Center for computing Services is planning on conducting a test of the plan NLT August 06.

Condition: Data Backup and Off-site Storage. (Finding # E)

Controls over data backup and off-site storage were not in place and did not fully comply with DoD policy. This occurred because CS had not developed adequate management controls to effectively manage data backups and off-site storage. Thirteen of 16 sites did not have adequate procedures to manage data backups and 9 of 16 off-sites facilities did not have adequate physical



and environmental controls. The lack of adequate guidance for data backup and storage could limit the ability for CS to restore operations and process essential data in a timely manner.

E.1.a DoD IG recommends that the Director, Center for Computing Services develop, implement, and test consistent data backup policies and procedures across all entity sites. These policies and procedures should include:

A process for appropriately marking and cataloging recovery data.

Center for Computing Services Response: Concur. Center for Computing Services has established a process for appropriately marking and cataloging recovery data in accordance with the CSD Security Handbook (draft released February 06).

E.1.b DoD IG recommends that the Director, Center for Computing Services develop, implement, and test consistent data backup policies and procedures across all entity sites. These policies and procedures should include:

A process to periodically test data backups to ensure timely recovery in the event of a service interruption or emergency.

Center for Computing Services Response: Concur. Center for Computing Services uses Veritas Tape backup system, which does a bit for bit test of data that is backed up for all systems. CSD has established a process to periodically test data backups to ensure timely recovery in the event of a service interruption or emergency for customers that provide backup servers or LPAR's in accordance with the SLA.

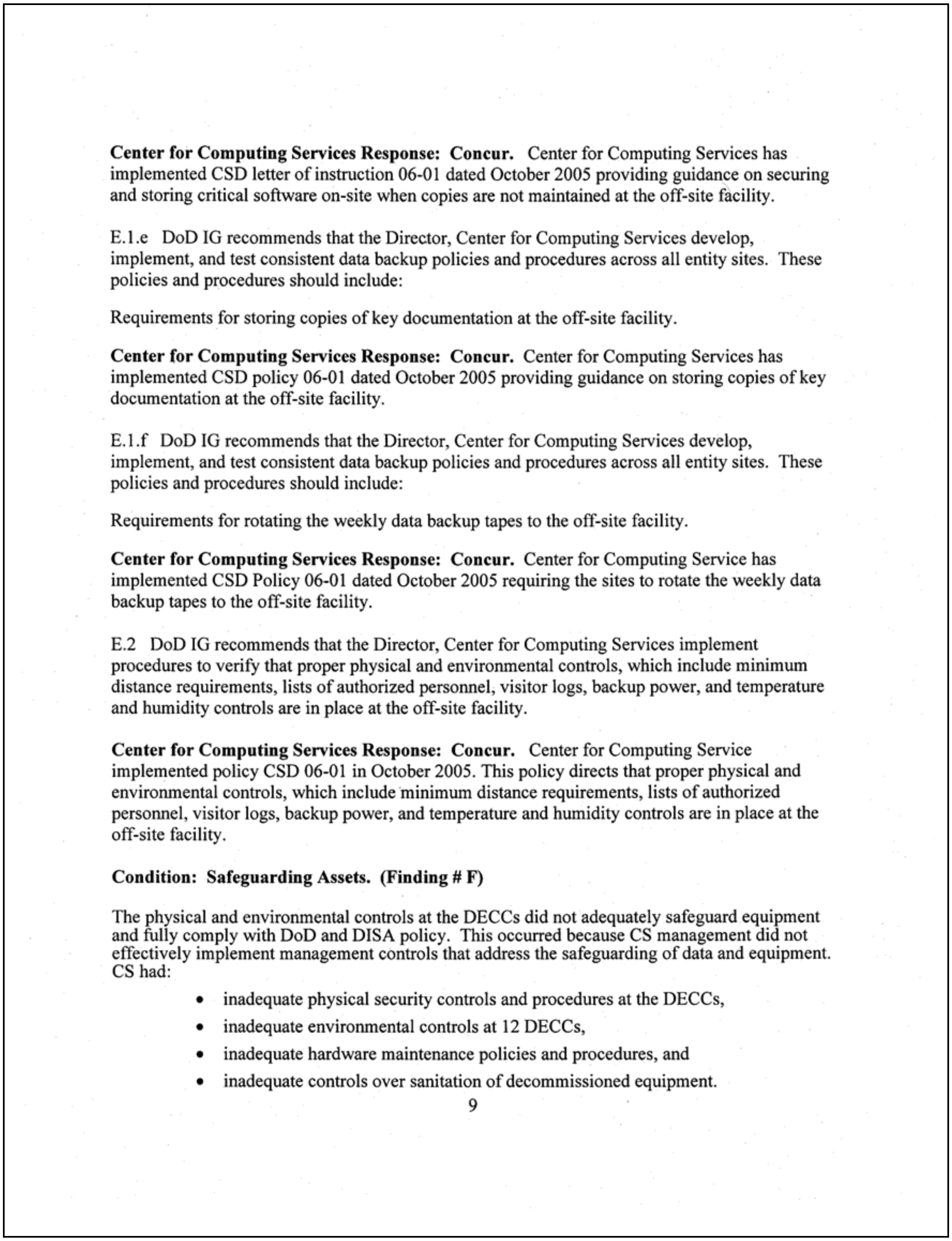
E.1.c DoD IG recommends that the Director, Center for Computing Services develop, implement, and test consistent data backup policies and procedures across all entity sites. These policies and procedures should include:

Consistent physical control over backup tapes when transporting to and from the off-site facility.

Center for Computing Services Response: Concur. Center for Computing Service has implemented CSD Policy 06-01 dated October 2005 directing the sites to have consistent physical control over backup tapes while the backup tapes are being transported to and from the off–site storage facility.

E.1.d DoD IG recommends that the Director, Center for Computing Services develop, implement, and test consistent data backup policies and procedures across all entity sites. These policies and procedures should include:

Standards for securing and storing critical software on-site when copies are not maintained at the off-site facility.



Center for Computing Services Response: Concur. Center for Computing Services has implemented CSD letter of instruction 06-01 dated October 2005 providing guidance on securing and storing critical software on-site when copies are not maintained at the off-site facility.

E.1.e DoD IG recommends that the Director, Center for Computing Services develop, implement, and test consistent data backup policies and procedures across all entity sites. These policies and procedures should include:

Requirements for storing copies of key documentation at the off-site facility.

Center for Computing Services Response: Concur. Center for Computing Services has implemented CSD policy 06-01 dated October 2005 providing guidance on storing copies of key documentation at the off-site facility.

E.1.f DoD IG recommends that the Director, Center for Computing Services develop, implement, and test consistent data backup policies and procedures across all entity sites. These policies and procedures should include:

Requirements for rotating the weekly data backup tapes to the off-site facility.

Center for Computing Services Response: Concur. Center for Computing Service has implemented CSD Policy 06-01 dated October 2005 requiring the sites to rotate the weekly data backup tapes to the off-site facility.

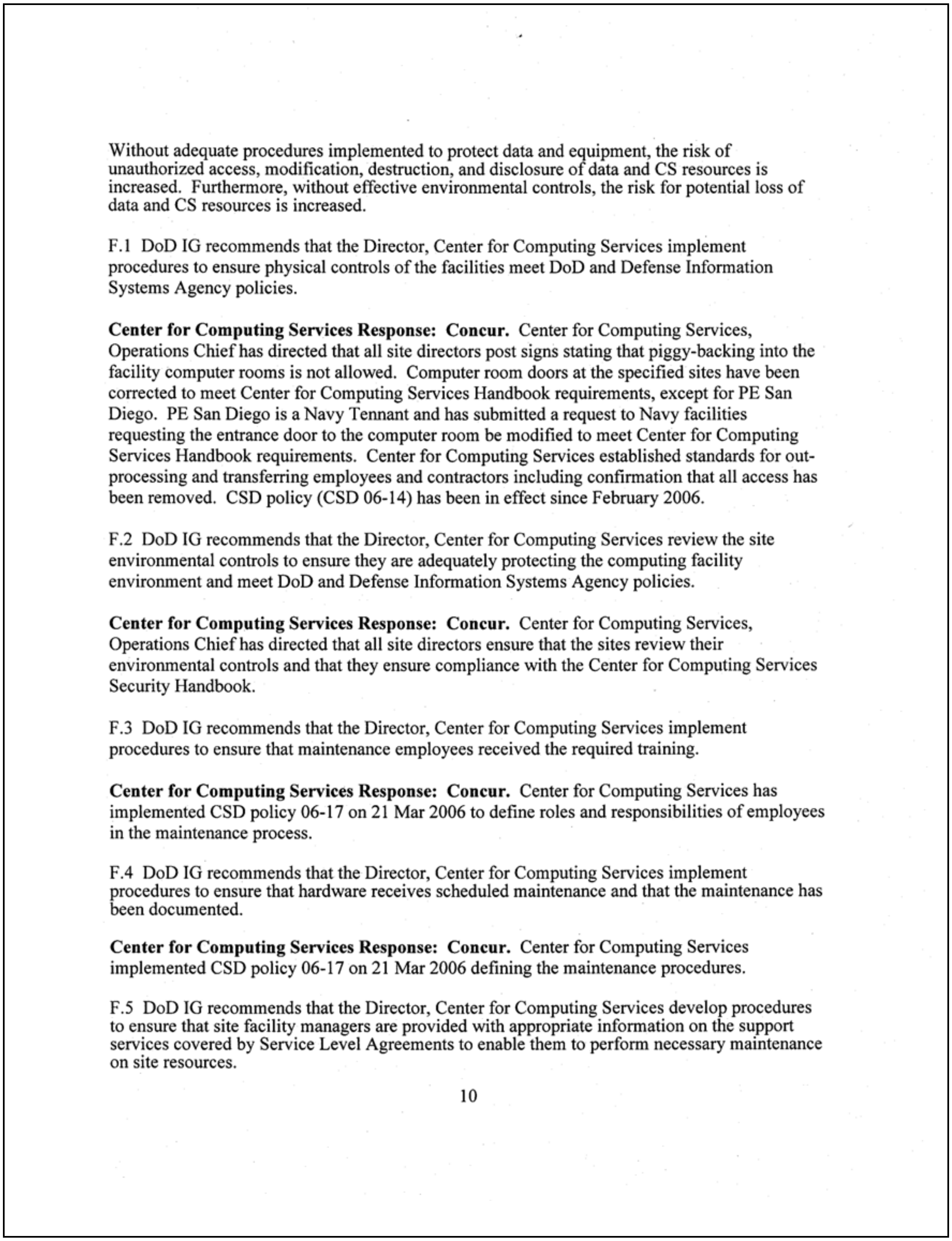
E.2 DoD IG recommends that the Director, Center for Computing Services implement procedures to verify that proper physical and environmental controls, which include minimum distance requirements, lists of authorized personnel, visitor logs, backup power, and temperature and humidity controls are in place at the off-site facility.

Center for Computing Services Response: Concur. Center for Computing Service implemented policy CSD 06-01 in October 2005. This policy directs that proper physical and environmental controls, which include minimum distance requirements, lists of authorized personnel, visitor logs, backup power, and temperature and humidity controls are in place at the off-site facility.

Condition: Safeguarding Assets. (Finding # F)

The physical and environmental controls at the DECCs did not adequately safeguard equipment and fully comply with DoD and DISA policy. This occurred because CS management did not effectively implement management controls that address the safeguarding of data and equipment. CS had:

- inadequate physical security controls and procedures at the DECCs,
- inadequate environmental controls at 12 DECCs,
- inadequate hardware maintenance policies and procedures, and
- inadequate controls over sanitation of decommissioned equipment.



Without adequate procedures implemented to protect data and equipment, the risk of unauthorized access, modification, destruction, and disclosure of data and CS resources is increased. Furthermore, without effective environmental controls, the risk for potential loss of data and CS resources is increased.

F.1 DoD IG recommends that the Director, Center for Computing Services implement procedures to ensure physical controls of the facilities meet DoD and Defense Information Systems Agency policies.

Center for Computing Services Response: Concur. Center for Computing Services, Operations Chief has directed that all site directors post signs stating that piggy-backing into the facility computer rooms is not allowed. Computer room doors at the specified sites have been corrected to meet Center for Computing Services Handbook requirements, except for PE San Diego. PE San Diego is a Navy Tennant and has submitted a request to Navy facilities requesting the entrance door to the computer room be modified to meet Center for Computing Services Handbook requirements. Center for Computing Services established standards for out-processing and transferring employees and contractors including confirmation that all access has been removed. CSD policy (CSD 06-14) has been in effect since February 2006.

F.2 DoD IG recommends that the Director, Center for Computing Services review the site environmental controls to ensure they are adequately protecting the computing facility environment and meet DoD and Defense Information Systems Agency policies.

Center for Computing Services Response: Concur. Center for Computing Services, Operations Chief has directed that all site directors ensure that the sites review their environmental controls and that they ensure compliance with the Center for Computing Services Security Handbook.

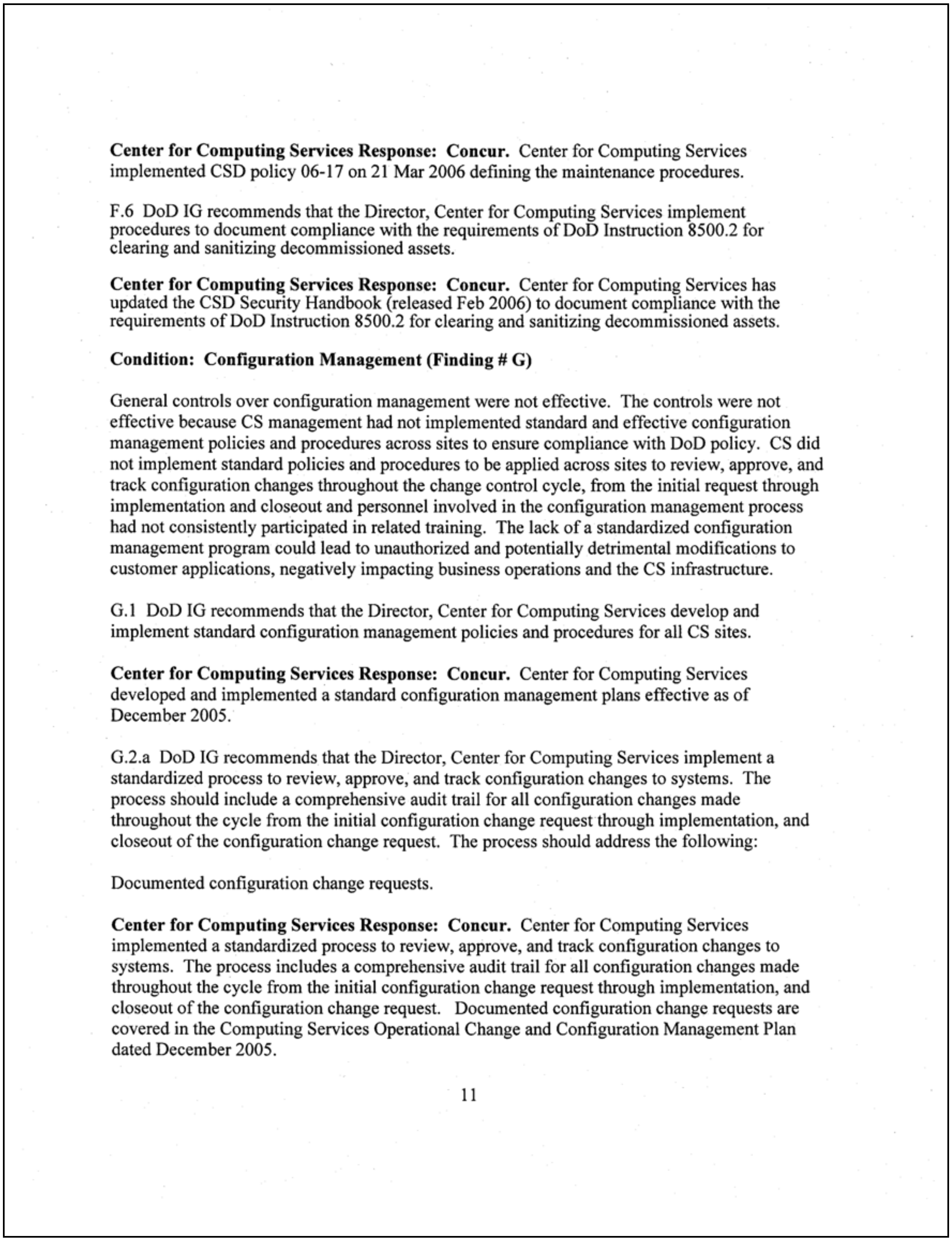
F.3 DoD IG recommends that the Director, Center for Computing Services implement procedures to ensure that maintenance employees received the required training.

Center for Computing Services Response: Concur. Center for Computing Services has implemented CSD policy 06-17 on 21 Mar 2006 to define roles and responsibilities of employees in the maintenance process.

F.4 DoD IG recommends that the Director, Center for Computing Services implement procedures to ensure that hardware receives scheduled maintenance and that the maintenance has been documented.

Center for Computing Services Response: Concur. Center for Computing Services implemented CSD policy 06-17 on 21 Mar 2006 defining the maintenance procedures.

F.5 DoD IG recommends that the Director, Center for Computing Services develop procedures to ensure that site facility managers are provided with appropriate information on the support services covered by Service Level Agreements to enable them to perform necessary maintenance on site resources.



Center for Computing Services Response: Concur. Center for Computing Services implemented CSD policy 06-17 on 21 Mar 2006 defining the maintenance procedures.

F.6 DoD IG recommends that the Director, Center for Computing Services implement procedures to document compliance with the requirements of DoD Instruction 8500.2 for clearing and sanitizing decommissioned assets.

Center for Computing Services Response: Concur. Center for Computing Services has updated the CSD Security Handbook (released Feb 2006) to document compliance with the requirements of DoD Instruction 8500.2 for clearing and sanitizing decommissioned assets.

Condition: Configuration Management (Finding # G)

General controls over configuration management were not effective. The controls were not effective because CS management had not implemented standard and effective configuration management policies and procedures across sites to ensure compliance with DoD policy. CS did not implement standard policies and procedures to be applied across sites to review, approve, and track configuration changes throughout the change control cycle, from the initial request through implementation and closeout and personnel involved in the configuration management process had not consistently participated in related training. The lack of a standardized configuration management program could lead to unauthorized and potentially detrimental modifications to customer applications, negatively impacting business operations and the CS infrastructure.

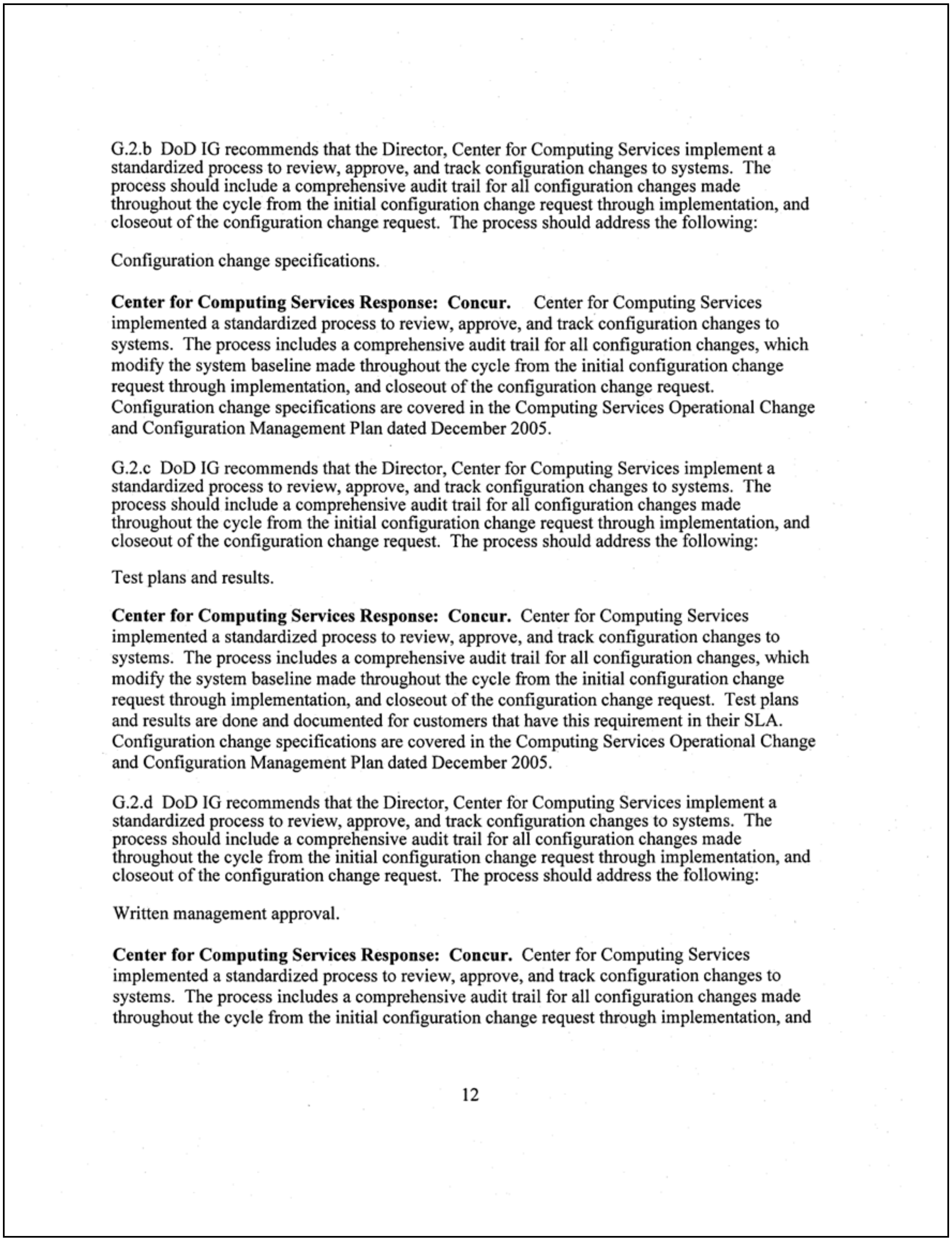
G.1 DoD IG recommends that the Director, Center for Computing Services develop and implement standard configuration management policies and procedures for all CS sites.

Center for Computing Services Response: Concur. Center for Computing Services developed and implemented a standard configuration management plans effective as of December 2005.

G.2.a DoD IG recommends that the Director, Center for Computing Services implement a standardized process to review, approve, and track configuration changes to systems. The process should include a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. The process should address the following:

Documented configuration change requests.

Center for Computing Services Response: Concur. Center for Computing Services implemented a standardized process to review, approve, and track configuration changes to systems. The process includes a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. Documented configuration change requests are covered in the Computing Services Operational Change and Configuration Management Plan dated December 2005.



G.2.b DoD IG recommends that the Director, Center for Computing Services implement a standardized process to review, approve, and track configuration changes to systems. The process should include a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. The process should address the following:

Configuration change specifications.

Center for Computing Services Response: Concur. Center for Computing Services implemented a standardized process to review, approve, and track configuration changes to systems. The process includes a comprehensive audit trail for all configuration changes, which modify the system baseline made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. Configuration change specifications are covered in the Computing Services Operational Change and Configuration Management Plan dated December 2005.

G.2.c DoD IG recommends that the Director, Center for Computing Services implement a standardized process to review, approve, and track configuration changes to systems. The process should include a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. The process should address the following:

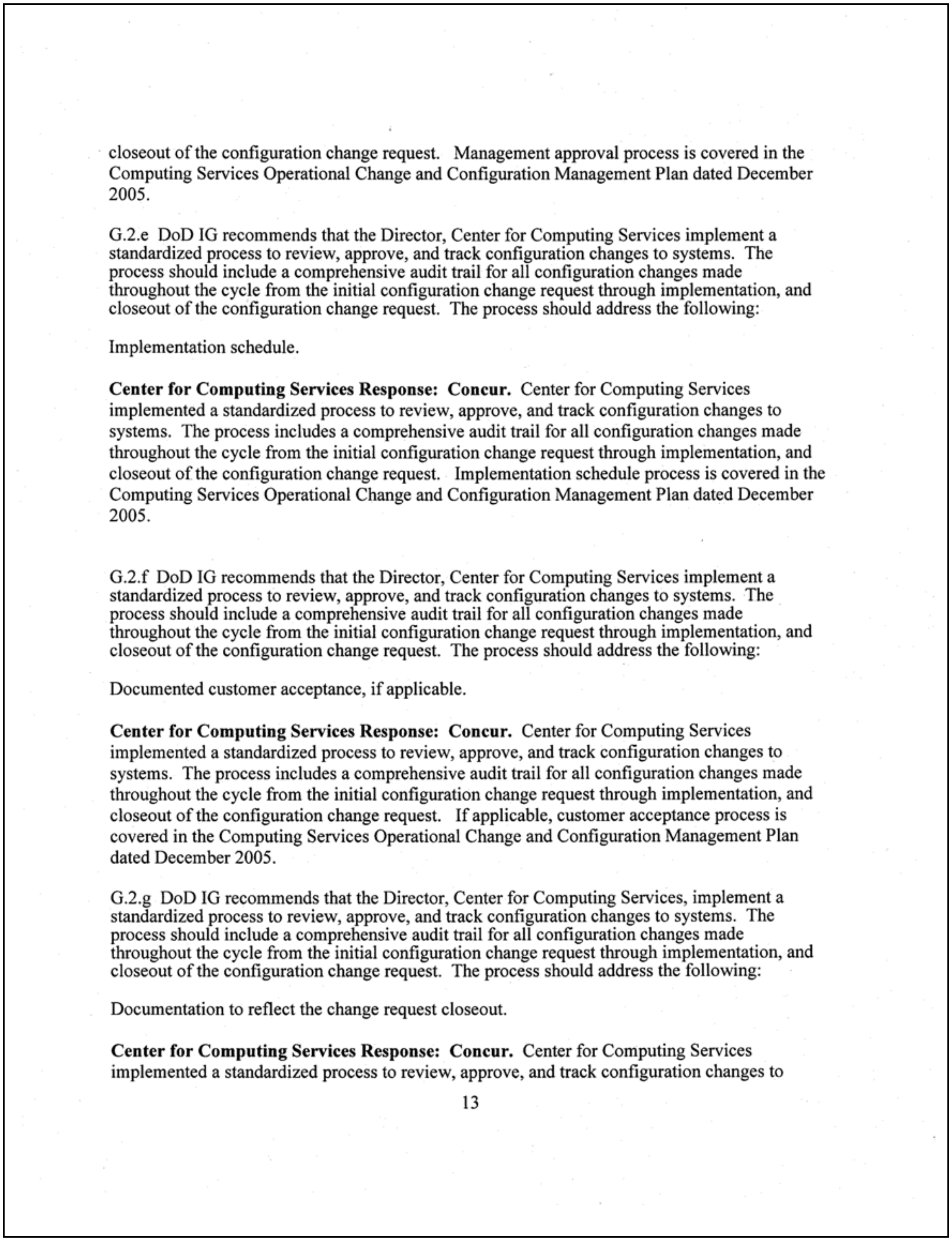
Test plans and results.

Center for Computing Services Response: Concur. Center for Computing Services implemented a standardized process to review, approve, and track configuration changes to systems. The process includes a comprehensive audit trail for all configuration changes, which modify the system baseline made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. Test plans and results are done and documented for customers that have this requirement in their SLA. Configuration change specifications are covered in the Computing Services Operational Change and Configuration Management Plan dated December 2005.

G.2.d DoD IG recommends that the Director, Center for Computing Services implement a standardized process to review, approve, and track configuration changes to systems. The process should include a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. The process should address the following:

Written management approval.

Center for Computing Services Response: Concur. Center for Computing Services implemented a standardized process to review, approve, and track configuration changes to systems. The process includes a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and



closeout of the configuration change request. Management approval process is covered in the Computing Services Operational Change and Configuration Management Plan dated December 2005.

G.2.e DoD IG recommends that the Director, Center for Computing Services implement a standardized process to review, approve, and track configuration changes to systems. The process should include a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. The process should address the following:

Implementation schedule.

Center for Computing Services Response: Concur. Center for Computing Services implemented a standardized process to review, approve, and track configuration changes to systems. The process includes a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. Implementation schedule process is covered in the Computing Services Operational Change and Configuration Management Plan dated December 2005.

G.2.f DoD IG recommends that the Director, Center for Computing Services implement a standardized process to review, approve, and track configuration changes to systems. The process should include a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. The process should address the following:

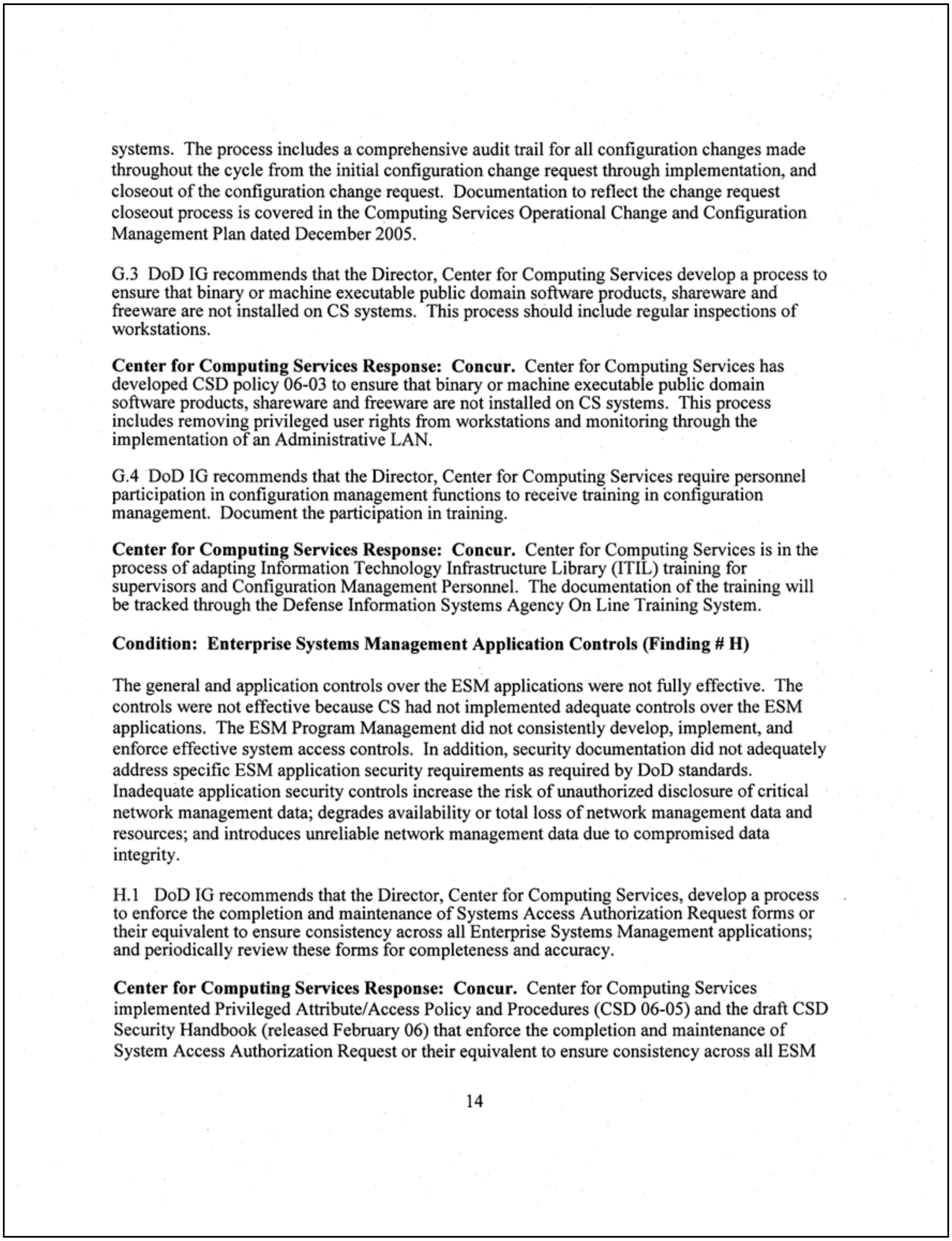
Documented customer acceptance, if applicable.

Center for Computing Services Response: Concur. Center for Computing Services implemented a standardized process to review, approve, and track configuration changes to systems. The process includes a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. If applicable, customer acceptance process is covered in the Computing Services Operational Change and Configuration Management Plan dated December 2005.

G.2.g DoD IG recommends that the Director, Center for Computing Services, implement a standardized process to review, approve, and track configuration changes to systems. The process should include a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. The process should address the following:

Documentation to reflect the change request closeout.

Center for Computing Services Response: Concur. Center for Computing Services implemented a standardized process to review, approve, and track configuration changes to



systems. The process includes a comprehensive audit trail for all configuration changes made throughout the cycle from the initial configuration change request through implementation, and closeout of the configuration change request. Documentation to reflect the change request closeout process is covered in the Computing Services Operational Change and Configuration Management Plan dated December 2005.

G.3 DoD IG recommends that the Director, Center for Computing Services develop a process to ensure that binary or machine executable public domain software products, shareware and freeware are not installed on CS systems. This process should include regular inspections of workstations.

Center for Computing Services Response: Concur. Center for Computing Services has developed CSD policy 06-03 to ensure that binary or machine executable public domain software products, shareware and freeware are not installed on CS systems. This process includes removing privileged user rights from workstations and monitoring through the implementation of an Administrative LAN.

G.4 DoD IG recommends that the Director, Center for Computing Services require personnel participation in configuration management functions to receive training in configuration management. Document the participation in training.

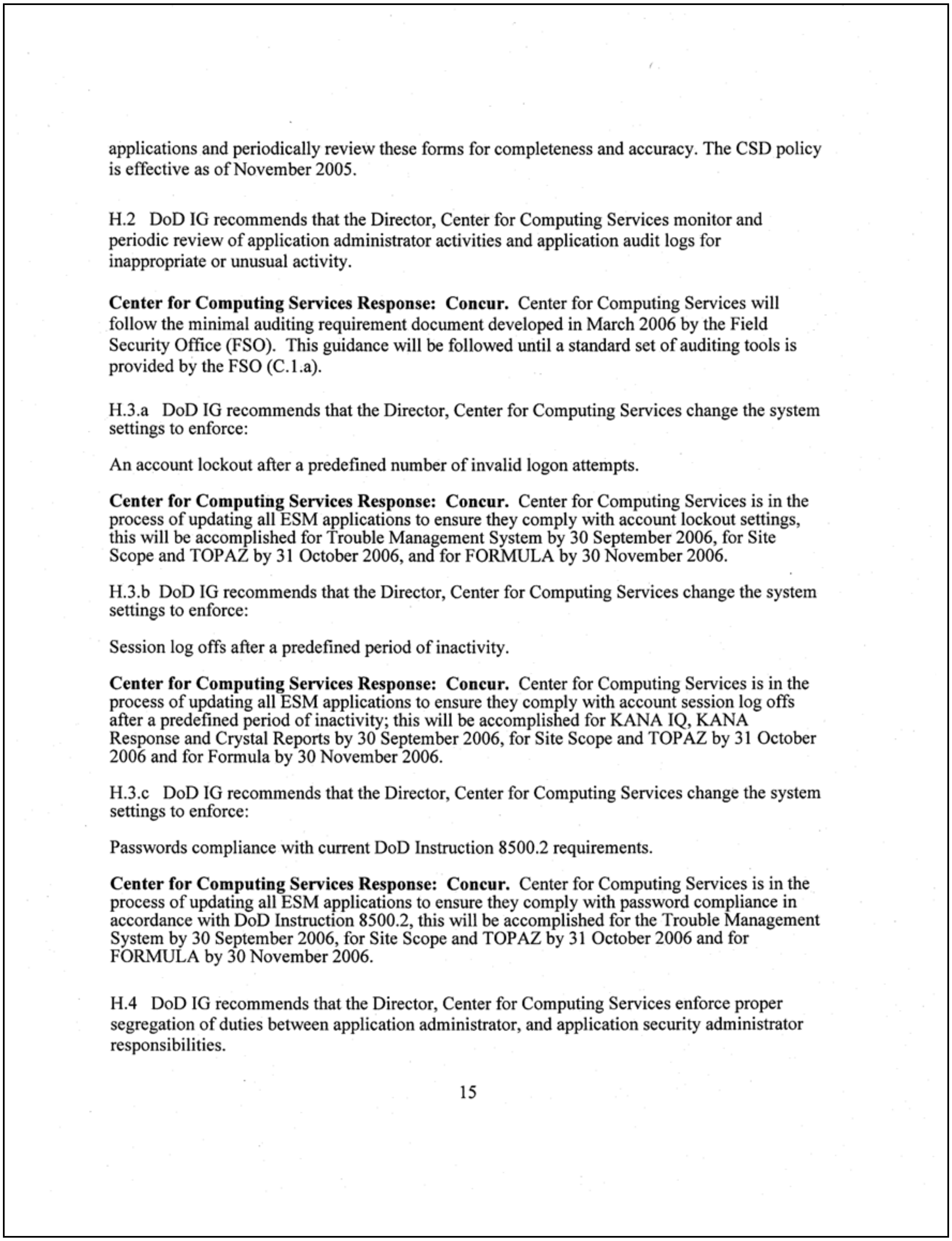
Center for Computing Services Response: Concur. Center for Computing Services is in the process of adapting Information Technology Infrastructure Library (ITIL) training for supervisors and Configuration Management Personnel. The documentation of the training will be tracked through the Defense Information Systems Agency On Line Training System.

Condition: Enterprise Systems Management Application Controls (Finding # H)

The general and application controls over the ESM applications were not fully effective. The controls were not effective because CS had not implemented adequate controls over the ESM applications. The ESM Program Management did not consistently develop, implement, and enforce effective system access controls. In addition, security documentation did not adequately address specific ESM application security requirements as required by DoD standards. Inadequate application security controls increase the risk of unauthorized disclosure of critical network management data; degrades availability or total loss of network management data and resources; and introduces unreliable network management data due to compromised data integrity.

H.1 DoD IG recommends that the Director, Center for Computing Services, develop a process to enforce the completion and maintenance of Systems Access Authorization Request forms or their equivalent to ensure consistency across all Enterprise Systems Management applications; and periodically review these forms for completeness and accuracy.

Center for Computing Services Response: Concur. Center for Computing Services implemented Privileged Attribute/Access Policy and Procedures (CSD 06-05) and the draft CSD Security Handbook (released February 06) that enforce the completion and maintenance of System Access Authorization Request or their equivalent to ensure consistency across all ESM



applications and periodically review these forms for completeness and accuracy. The CSD policy is effective as of November 2005.

H.2 DoD IG recommends that the Director, Center for Computing Services monitor and periodic review of application administrator activities and application audit logs for inappropriate or unusual activity.

Center for Computing Services Response: Concur. Center for Computing Services will follow the minimal auditing requirement document developed in March 2006 by the Field Security Office (FSO). This guidance will be followed until a standard set of auditing tools is provided by the FSO (C.1.a).

H.3.a DoD IG recommends that the Director, Center for Computing Services change the system settings to enforce:

An account lockout after a predefined number of invalid logon attempts.

Center for Computing Services Response: Concur. Center for Computing Services is in the process of updating all ESM applications to ensure they comply with account lockout settings, this will be accomplished for Trouble Management System by 30 September 2006, for Site Scope and TOPAZ by 31 October 2006, and for FORMULA by 30 November 2006.

H.3.b DoD IG recommends that the Director, Center for Computing Services change the system settings to enforce:

Session log offs after a predefined period of inactivity.

Center for Computing Services Response: Concur. Center for Computing Services is in the process of updating all ESM applications to ensure they comply with account session log offs after a predefined period of inactivity; this will be accomplished for KANA IQ, KANA Response and Crystal Reports by 30 September 2006, for Site Scope and TOPAZ by 31 October 2006 and for Formula by 30 November 2006.

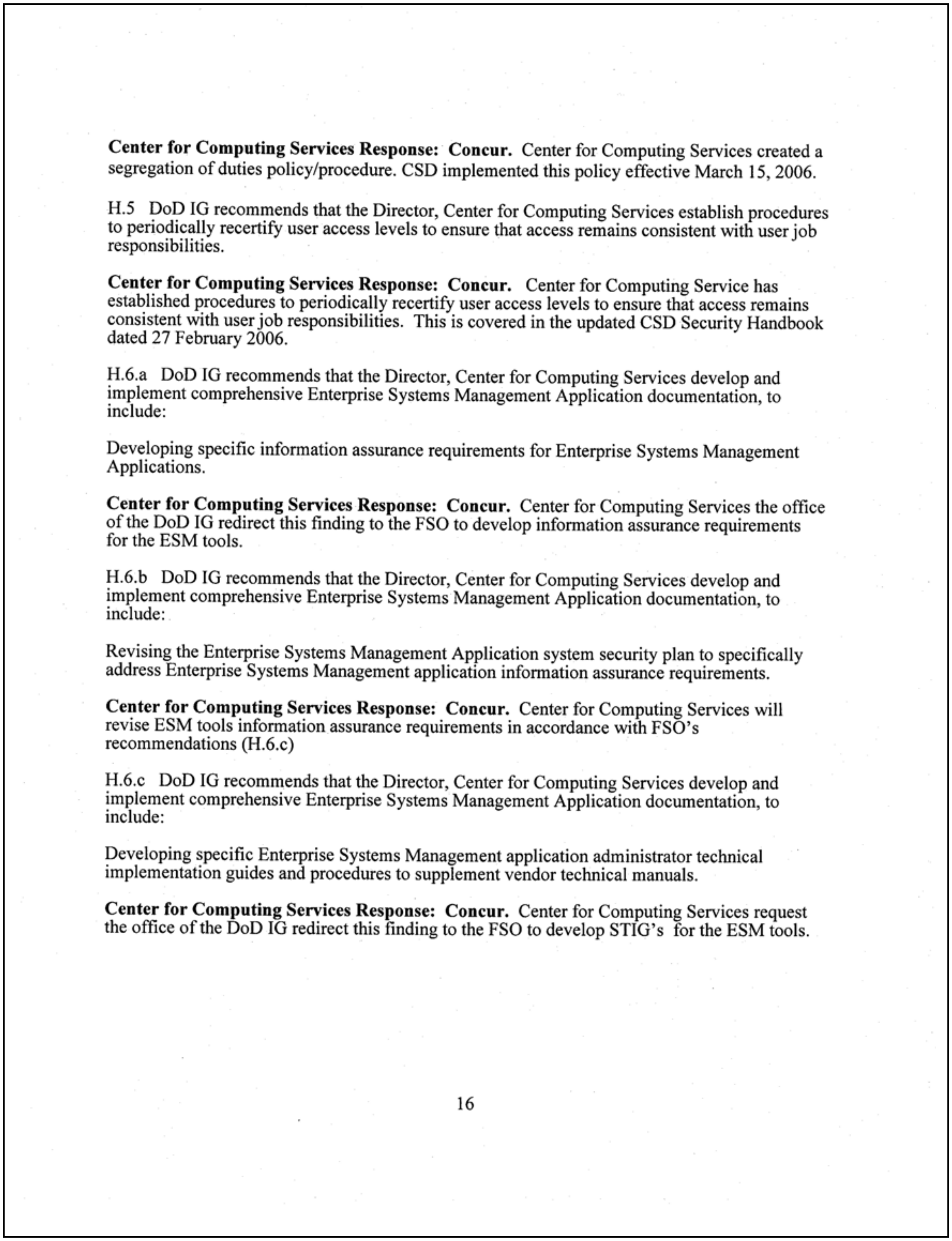
H.3.c DoD IG recommends that the Director, Center for Computing Services change the system settings to enforce:

Passwords compliance with current DoD Instruction 8500.2 requirements.

Center for Computing Services Response: Concur. Center for Computing Services is in the process of updating all ESM applications to ensure they comply with password compliance in accordance with DoD Instruction 8500.2, this will be accomplished for the Trouble Management System by 30 September 2006, for Site Scope and TOPAZ by 31 October 2006 and for FORMULA by 30 November 2006.

H.4 DoD IG recommends that the Director, Center for Computing Services enforce proper segregation of duties between application administrator, and application security administrator responsibilities.

Final Report
Reference



Center for Computing Services Response: Concur. Center for Computing Services created a segregation of duties policy/procedure. CSD implemented this policy effective March 15, 2006.

H.5 DoD IG recommends that the Director, Center for Computing Services establish procedures to periodically recertify user access levels to ensure that access remains consistent with user job responsibilities.

Center for Computing Services Response: Concur. Center for Computing Service has established procedures to periodically recertify user access levels to ensure that access remains consistent with user job responsibilities. This is covered in the updated CSD Security Handbook dated 27 February 2006.

H.6.a DoD IG recommends that the Director, Center for Computing Services develop and implement comprehensive Enterprise Systems Management Application documentation, to include: H.7.a

Developing specific information assurance requirements for Enterprise Systems Management Applications.

Center for Computing Services Response: Concur. Center for Computing Services the office of the DoD IG redirect this finding to the FSO to develop information assurance requirements for the ESM tools.

H.6.b DoD IG recommends that the Director, Center for Computing Services develop and implement comprehensive Enterprise Systems Management Application documentation, to include: H.6

Revising the Enterprise Systems Management Application system security plan to specifically address Enterprise Systems Management application information assurance requirements.

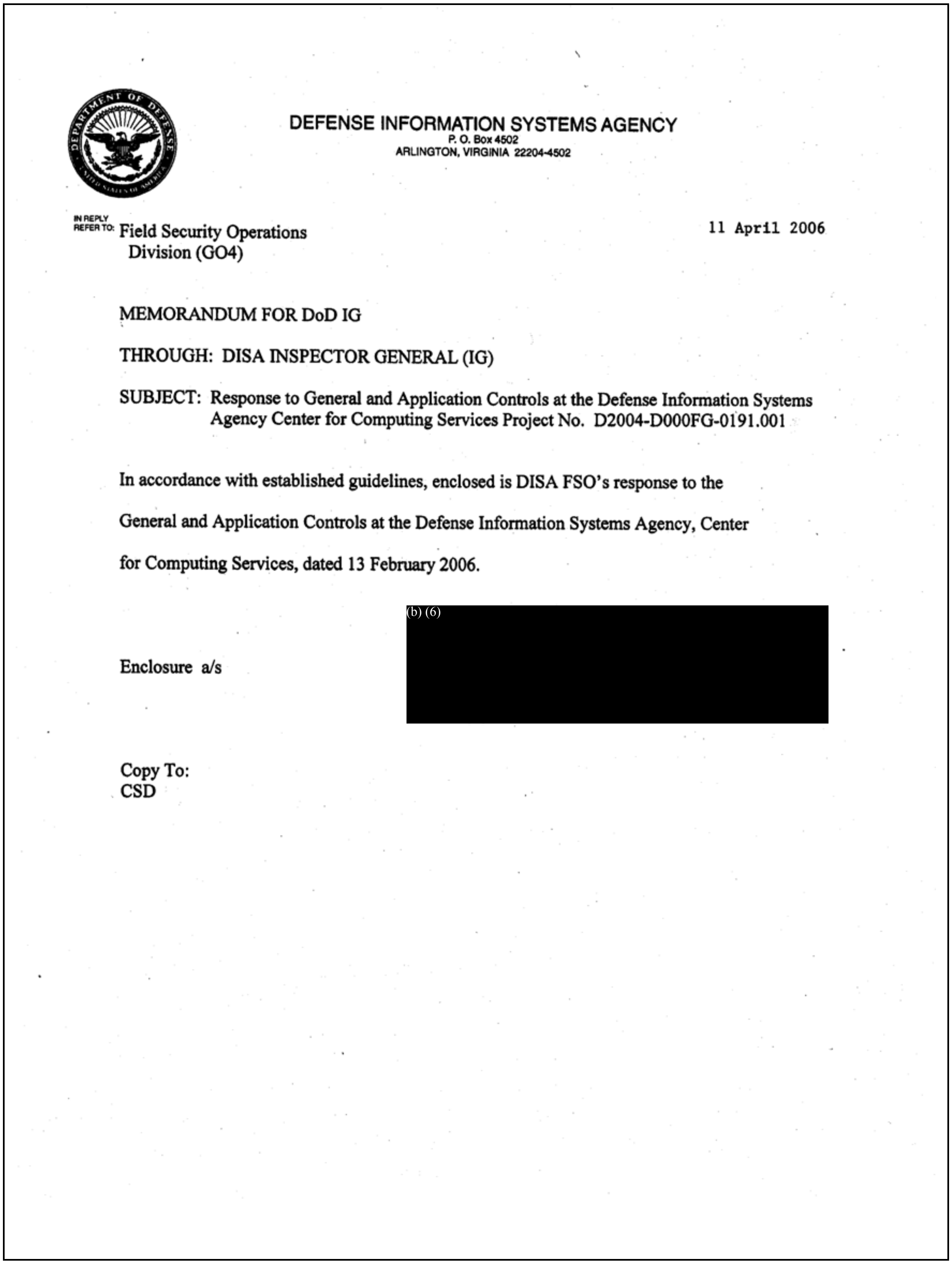
Center for Computing Services Response: Concur. Center for Computing Services will revise ESM tools information assurance requirements in accordance with FSO's recommendations (H.6.c)

H.6.c DoD IG recommends that the Director, Center for Computing Services develop and implement comprehensive Enterprise Systems Management Application documentation, to include: H.7.b

Developing specific Enterprise Systems Management application administrator technical implementation guides and procedures to supplement vendor technical manuals.

Center for Computing Services Response: Concur. Center for Computing Services request the office of the DoD IG redirect this finding to the FSO to develop STIG's for the ESM tools.

Defense Information Systems Agency, Field Security Operations Comments



DEFENSE INFORMATION SYSTEMS AGENCY
P. O. Box 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY
REFER TO: Field Security Operations
Division (GO4)

11 April 2006

MEMORANDUM FOR DoD IG

THROUGH: DISA INSPECTOR GENERAL (IG)

SUBJECT: Response to General and Application Controls at the Defense Information Systems Agency Center for Computing Services Project No. D2004-D000FG-0191.001

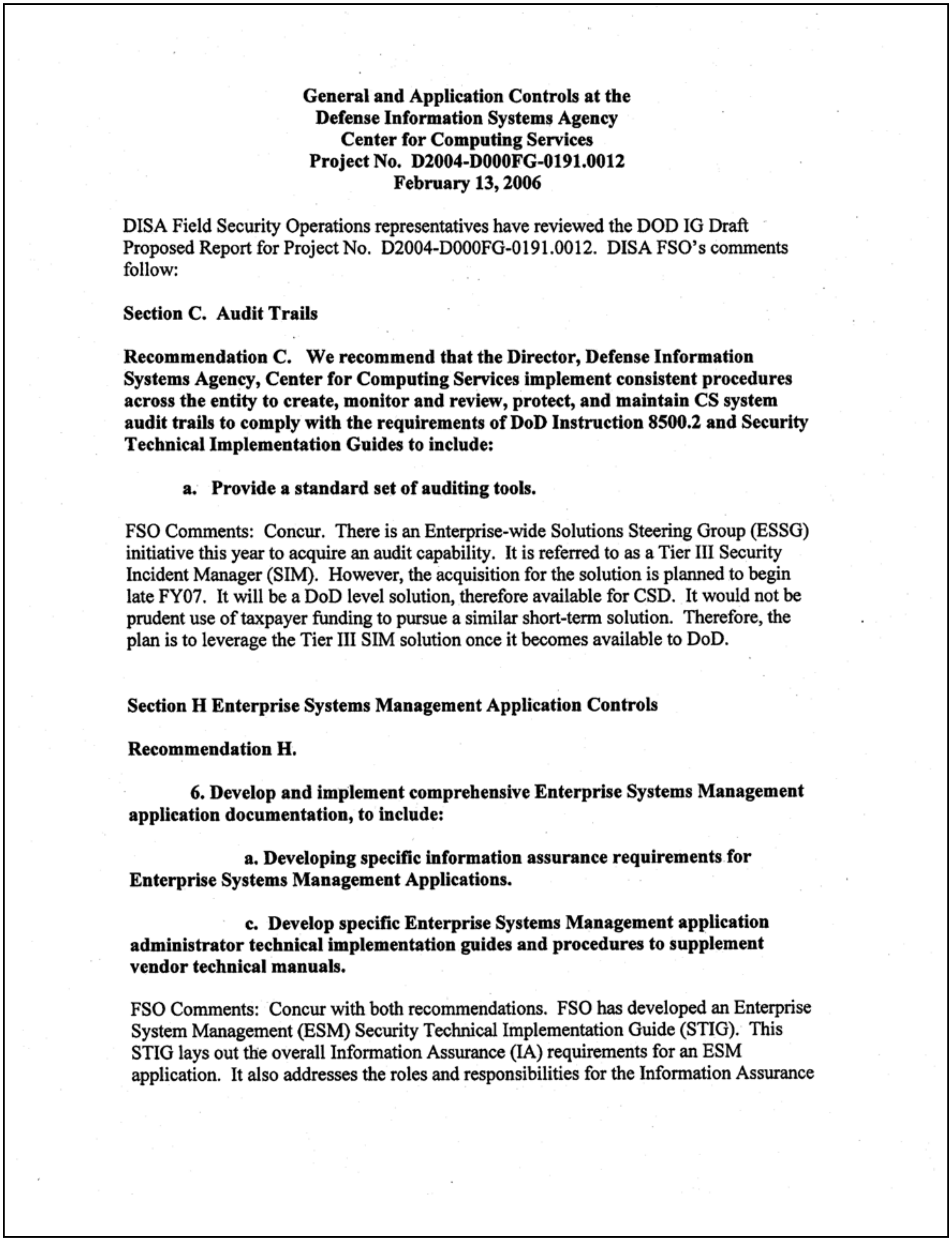
In accordance with established guidelines, enclosed is DISA FSO's response to the General and Application Controls at the Defense Information Systems Agency, Center for Computing Services, dated 13 February 2006.

(b) (6)

Enclosure a/s

Copy To:
CSD

Final Report
Reference



General and Application Controls at the
Defense Information Systems Agency
Center for Computing Services
Project No. D2004-D000FG-0191.0012
February 13, 2006

DISA Field Security Operations representatives have reviewed the DOD IG Draft Proposed Report for Project No. D2004-D000FG-0191.0012. DISA FSO's comments follow:

Section C. Audit Trails

Recommendation C. We recommend that the Director, Defense Information Systems Agency, Center for Computing Services implement consistent procedures across the entity to create, monitor and review, protect, and maintain CS system audit trails to comply with the requirements of DoD Instruction 8500.2 and Security Technical Implementation Guides to include:

C.2 **a. Provide a standard set of auditing tools.**

FSO Comments: Concur. There is an Enterprise-wide Solutions Steering Group (ESSG) initiative this year to acquire an audit capability. It is referred to as a Tier III Security Incident Manager (SIM). However, the acquisition for the solution is planned to begin late FY07. It will be a DoD level solution, therefore available for CSD. It would not be prudent use of taxpayer funding to pursue a similar short-term solution. Therefore, the plan is to leverage the Tier III SIM solution once it becomes available to DoD.

Section H Enterprise Systems Management Application Controls

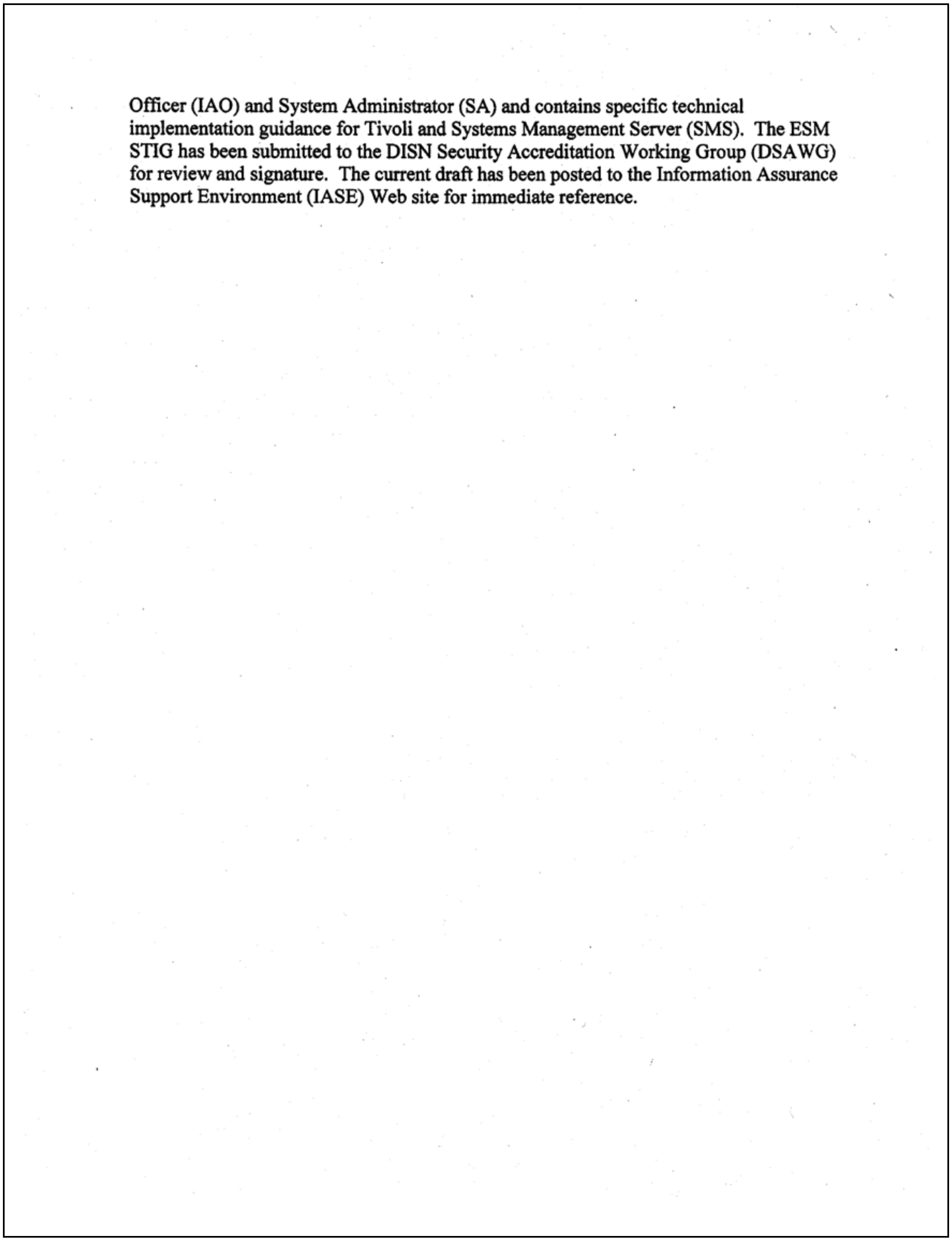
Recommendation H.

H.7 **6. Develop and implement comprehensive Enterprise Systems Management application documentation, to include:**

H.7.a **a. Developing specific information assurance requirements for Enterprise Systems Management Applications.**

H.7.b **c. Develop specific Enterprise Systems Management application administrator technical implementation guides and procedures to supplement vendor technical manuals.**

FSO Comments: Concur with both recommendations. FSO has developed an Enterprise System Management (ESM) Security Technical Implementation Guide (STIG). This STIG lays out the overall Information Assurance (IA) requirements for an ESM application. It also addresses the roles and responsibilities for the Information Assurance



Officer (IAO) and System Administrator (SA) and contains specific technical implementation guidance for Tivoli and Systems Management Server (SMS). The ESM STIG has been submitted to the DISN Security Accreditation Working Group (DSAWG) for review and signature. The current draft has been posted to the Information Assurance Support Environment (IASE) Web site for immediate reference.

Team Members

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

Paul J. Granetto

(b) (6)

[redacted]