Report No. D-2007-082 April 9, 2007

Inspector General
United States
Department of Defense

Defense Information Systems Agency Controls over the Center for Computing Services

Additional Copies

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

Suggestions for Future Audits

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

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

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

April 9, 2007

MEMORANDUM FOR DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on the Defense Information Systems Agency Controls over the Center for Computing Services (Report No. D-2007-082)

We are providing this report for review and comment. We considered comments from the Defense Information Systems Agency Chief Information Officer, Center for Computing Services, and Field Security Operations when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Defense Information Systems Agency Chief Information Officer comments were partially responsive. Therefore, we request that the Defense Information Systems Agency Chief Information Officer provide additional comments on Recommendation A.2 by May 9, 2007.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to Auddfs@dodig.mil. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Patricia C. Remington at (703) 428-1054 (DSN 328-1054) or Ms. Suzette L. Luecke at (703) 428-1067 (DSN 328-1067). See Appendix G for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

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

Department of Defense Office of Inspector General

Report No. D-2007-082 **April 9, 2007**
(Project No. D2006-D000FG-0053.001)

The Defense Information Systems Agency Controls over the 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 (DISA), Center for Computing Services (CS) may find this report of interest, as will other CS user organizations and their independent auditors. Supervisors of any part of the DoD Information Assurance program may also find this report useful. This report supports the overall Statement on Auditing Standards No. 70 audit and describes compliance with general and application control objectives and compliance with applicable laws and regulations, including the DoD Information Technology Security Certification and Accreditation Process and the Security Technical Implementation Guides.

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 (Public Law 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 the 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. 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 Security Technical Implementation Guides, training program, information assurance program, and Defense Enterprise Computing Center Pacific needed improvement to ensure that information systems operated effectively and provided appropriate confidentiality, integrity, and availability for the systems located there. Without proper general and application controls in place, DISA may not safeguard data; protect computer application programs; preclude unauthorized access to system software and computing facilities; help to ensure continued computer operation in case of unexpected interruptions; and effectively manage, operate, and secure the computing environment; consequently, impacting security across the DoD environment. Specifically:

- CS had ineffective processes for managing computing device configuration in accordance with the DoD Security Technical Implementation Guides. DISA needs to provide an effective security readiness review mechanism and properly manage all vulnerabilities. See finding A of the report for detailed recommendations.

- DISA did not effectively and consistently monitor information assurance training and system administrator certification requirements for all personnel. DISA needs to improve the process of managing and tracking all training and certification requirements and completions. See finding B of the report for detailed recommendations.

- DISA needs to establish a more comprehensive and integrated information assurance program. See finding C of the report for detailed recommendations.

- The general controls over Defense Enterprise Computing Center Pacific were not effective. CS needs to enforce the applicable DoD and DISA policies on Defense Enterprise Computing Center Pacific. See finding D of the report for detailed recommendations.

Management Comments and Audit Response. The DISA Chief Information Officer concurred with 2 recommendations and nonconcurred with 1 recommendation; the Director, CS concurred with 20 recommendations and nonconcurred with 1 recommendation; and the Chief, Field Security Operations concurred with 1 recommendation. We agree with the actions proposed by the DISA Chief Information Officer but request additional details on the actions. We request that the DISA Chief Information Officer provide comments on the final report by May 9, 2007. See the Finding section of the report for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.

Table of Contents

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, DISA operates 1,400 applications in 18 geographically separate facilities using approximately 40 mainframes and more than 3,000 servers.

CS processing facilities, which are Defense Enterprise Computing Centers (DECCs), encompass 16 locations across the continental United States, as well as two overseas locations, Pearl Harbor, Hawaii, and Stuttgart, Germany. 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. DECC personnel responsibilities include production operations, such as site operating functions that directly support customer requirements, as well as technical and customer support functions. The 16 continental United States DECCs are divided into the following three functional designations.

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

- Infrastructure Services Centers. The Infrastructure Services Centers perform system management for specialized fielding efforts from CS customers. The Infrastructure Services Centers 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. The Processing Elements 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 to provide centralized network management for all DECCs. The Communications Control Centers support all routing, switching, domain name servers, wide-area network connectivity to DISA Network Services, and network security device

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

operations. The Communications Control Centers are co-located with DECCs Montgomery and Oklahoma City.

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 lay 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 systems, and
- manage changes to an established baseline in a secure manner.

The DoD Instruction 8500.2 defines mission assurance categories (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. The 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. The confidentiality level is also used to establish interconnection controls and approvals and acceptable methods by which users may access a system, including intranet, Internet, and wireless access. The DoD Security Technical Implementation Guides (STIGs) are written for MAC II Sensitive systems. The MAC II Sensitive systems handle 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 that could adversely affect national interest or Federal programs.

Controls. Information technology (IT) controls are divided into two types of controls, general and application. 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. Application controls are directly related to individual computerized applications. These controls help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. General and application controls must be effective to help ensure the reliability, 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. The objective of the audit was to determine whether (1) DISA general controls over the CS are adequately designed and effective, (2) general and application controls for internal applications that support CS management are adequately designed and effective, and (3) CS is in compliance with applicable Federal and DoD IT and IA policies. See Appendix A for a discussion of the scope and methodology of our review. See Appendix B for prior coverage related to the objectives.

A. Security Technical Implementation Guides

The CS had ineffective processes for managing computing device configuration in accordance with the DoD STIGs. Specifically, the quality assurance process for the Security Readiness Review (SRR) toolkit was ineffective, CS did not properly manage all vulnerabilities, and DISA was still in the process of implementing several recommendations from previous reports. Non-compliance with the STIGs increases the risk of losing data confidentiality, system integrity, and system availability.

Security Configuration Guidelines

DoD Directive 8500.1 requires that all IA and IA-enabled IT products incorporated into DoD information systems be configured in accordance with DoD-approved security configuration guidelines. The Field Security Operations (FSO) develops system configuration guidelines, which are called the STIGs. The STIGs have become the foundation of translating the DoD IA requirements into technology-specific requirements.

All DISA assets are to be configured in accordance with the STIGs. The "Mandatory Information Assurance Guidance, DISA Computing Services Operations Policy Letter CS 05-09," August 31, 2005, establishes the minimum STIG compliance requirements for initial connection to the DoD network. Prior to system connection, a SRR must be performed in which the system is checked against manual procedures, automated scripts, and the FSO vulnerability scanning tool. The results from these assessments are uploaded into the Vulnerability Management System (VMS).

STIG Compliance

The CS had ineffective processes for ensuring and managing computing device configuration in accordance with the DoD STIGs. We used a statistical sample of computing devices, to test for STIG compliance and used the minimum system setting requirements established by the Mandatory Information Assurance Guidance to determine the pass or fail of the computing devices. The Mandatory Information Assurance Guidance requires that all Category I[2] findings be closed and that minimum closure rates be based on the operating system for Category II[3] findings. Table 1 contains the minimum closure rate for Category II findings.

[2] Category I findings are vulnerabilities that may result in a total loss of information and that provides an unauthorized person or software immediate access into a system, gains privileged access, bypasses a firewall, or results in a denial of service.

[3] Category II findings are vulnerabilities that provide information that has a high potential of giving access to an unauthorized person, or provide an unauthorized person the means to circumvent security controls.

Table 1. Category II Minimum Closure Rate	
Operating System	**Minimum Closure Rate**
Network	90%
IBM Mainframe	85%
UNIX	85%
Windows	90%

CS did not have effective processes to consistently or completely configure computing devices in accordance with STIGs. The following devices did not meet the minimum closure rates:

- All 19 of the IBM Mainframe,
- 7 of 15 Network,
- 5 of 46 UNIX, and
- 36 of 52 Windows devices.

For reporting purposes, we are only including results from the devices that we have performed substantive testing. Therefore, the total number of devices in the body of the report tested will differ from the total number used for statistical projection. See Appendix C for additional details on sampling approach and results.

In addition, we identified noncompliant trends in password and account management, system permissions, security settings, and baseline comparison. Many of these issues were identified in prior audit reports. See Appendix D for details on specific STIG-noncompliant items.

Configuration Compliance Management

The quality assurance process for the SRR toolkit was ineffective, CS did not properly manage all vulnerabilities, and DISA was still in the process of implementing several recommendations from previous audit reports. The lack of effective Windows and UNIX scripts hampers the ability of system administrators (SAs) to effectively manage security over computing devices and to adequately assess compliance with the STIGs. Additionally, the lack of visibility over the total number of vulnerabilities at the DECCs decreases DISA management's awareness of the actual security posture across DISA. Finally, without fully implementing prior year recommendations, there remains an increased risk of losing data confidentiality, system integrity, and system availability.

System Readiness Review Toolkit. The quality assurance process for the SRR toolkit released by FSO was not effective. The FSO develops scripts to test STIG compliance for various Windows and the UNIX devices on a quarterly basis. Once the FSO develops the scripts, the Systems Support Office (SSO) Montgomery, in conjunction with DECC Montgomery, performs a quality

assurance test of the Windows and UNIX scripts. The SSO Montgomery provides feedback to the FSO on the script issues identified during its quality assurance test and maintains issue logs. These issues identified for the UNIX script ranged from false positives and negatives, script syntax errors, and logic errors. The severity of these issues ranged from Category I to Category III.[4]

Based on the quality assurance test results, the FSO addresses as many of the identified issues as possible. After the FSO addresses the issues, the FSO sends the scripts back to the SSO Montgomery for customization. Once the scripts are customized for the DECCs, the SSO Montgomery releases the scripts to the DECCs. However, the customized scripts may still contain unresolved issues identified during the quality assurance test. For example, the quality assurance test log showed 50 outstanding UNIX script issues as of April 6, 2006. The FSO was not able to address all issues before releasing the scripts to the DECCs. The FSO needs to improve the quality assurance process to resolve the script issues prior to release.

Vulnerability Management. DISA did not effectively manage all vulnerabilities. The VMS reports on the security weaknesses and the associated corrective actions through Plan of Action and Milestones (POA&M) reports, which support the Federal Information Security Management Act of 2002 reporting requirements. The POA&M reports are used to identify and monitor IT security-related programmatic and system-level weaknesses found in programs and systems and serves as a baseline for assessing the maturity of the DoD IT security program. DISA prepared the high-level POA&M reports based on records maintained in the VMS. The POA&Ms are associated with each vulnerability, however, VMS did not include vulnerabilities identified by the DECC during self-assessments. Therefore, DISA may not have all the detailed information to provide aggregate POA&M reporting.

Process Improvement. During our audit, DISA was in the process of fully implementing recommendations from our previous audit reports. In prior reports, we recommended that the Director, CS develop a program to familiarize the SAs with their specific roles in maintaining a secure computing environment, including: a) specific STIG requirements that the SAs must comply with and b) specific guidance on how to manually test STIG requirements not tested by automated scripts. The FSO took over the responsibility of the SA Certification Program, but had not completed the training curriculum. DISA expects completion of this training by July 31, 2007.

Additionally, we recommended that the Director, CS disseminate and require the use of automated tools such as the Secure Configuration Compliance Validation Initiative and the Secure Configuration Remediation Initiative. As of December 4, 2006, CS was using the DoD enterprise solution of the Secure Configuration Compliance Validation Initiative and the Secure Configuration Remediation Initiative to implement recommendations in the following areas: passwords, services and protocols, peripheral devices, and configuration settings. However, CS does not expect to have them fully implemented until December 31, 2007.

[4] Category III findings are vulnerabilities that provide information that could lead to unauthorized access.

Recommendations, Management Comments, and Audit Response

A.1. We recommend that the Chief, Field Security Operations improve the quality assurance process to ensure that script issues are resolved and inform users of any unresolved issues or noncompliance with Security Technical Implementation Guide requirements.

Management Comments. The Chief, FSO concurred and stated that the FSO had taken proactive measures and implemented changes in the security tool development and release process. In addition, the FSO engaged the Joint Integration Testing Center to perform independent testing of the Gold Disk for the remainder of the FY 2007 releases and planned to expand this effort to include the FSO-developed scripts in FY 2008, based on availability of funding.

A.2. We recommend that the Director, Defense Information Systems Agency include all vulnerabilities, including those identified during self-assessments, with the appropriate Plan of Action and Milestone in the Vulnerability Management System.

Management Comments. The DISA Chief Information Officer and the Director, CS concurred. The Director, CS provided additional information indicating that DISA is in the process of implementing the DoD IA tools for the Information Assurance Vulnerability Alert and STIG compliance. He expects to implement the DoD IA tools by December 31, 2007.

Audit Response. Although the DISA Chief Information Officer and Director, CS concurred with the recommendation, implementing the DoD IA tools will not adequately ensure that vulnerabilities identified during self-assessments will be included in the Vulnerability Management System with the appropriate POA&M. Therefore, we ask that the DISA Chief Information Officer provide additional comments in response to the final report identifying specific actions that will account for vulnerabilities identified during self-assessments and the related POA&M.

B. Training

DISA did not effectively and consistently monitor IA Awareness training and SA certification requirements for all personnel because DISA had multiple organizations tracking training and certification completions. Without effective and consistent monitoring of training and certification activities, DISA is at risk that access to sensitive information may be inappropriately granted and DISA has little assurance that all SAs have the proper credentials to effectively manage the systems.

Training Requirements

DISA provides training and certification activities to personnel. DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, requires that:

- all authorized users of DoD information systems receive initial IA Awareness orientation as a condition of access and thereafter must complete annual IA Awareness training,
- privileged users and IA managers be fully qualified, trained, and certified to DoD baseline requirements to perform their IA duties,
- the status of the DoD Component IA certification and training be monitored and reported as an element of mission readiness and as a management review item, and
- the heads of DoD Components identify, document, and track IA personnel certifications and certification status.

Training Documentation

DISA did not effectively and consistently monitor IA Awareness training and SA certification requirements for all personnel. We selected a judgmental sample of 168 training records which show completion of IA Awareness training. Of the 168 records, DISA could not provide personnel training records for 26 of the sample items. See Table 2 for the details.

Table 2. IA Awareness Training Record		
Location	**Missing Record**	**Personnel Requested**
Columbus	0	4
Headquarters	0	9
Mechanicsburg	23	80
Montgomery	0	17
Ogden	0	41
Oklahoma City	0	11
Pacific	1	1
San Antonio	0	3
St. Louis	2	2
Total	**26**	**168**

Additionally, we selected a judgmental sample of 112 SA Certification training records. The FSO could not provide records for 25 of the 112 SAs to show completion of certifications. See Table 3 for the details.

Table 3. SA Certification Training Record		
Location	**Missing Record**	**SAs Sampled**
Columbus	0	14
Mechanicsburg	21	23
Montgomery	4	23
Ogden	0	12
Oklahoma City	0	38
San Antonio	0	1
St. Louis	0	1
Total	**25**	**112**

Training and Certification Monitoring

DISA used three organizations to document and track IA Awareness training and SA certification and each of these organizations used different systems. The Chief Information Office and Manpower, Personnel, and Security were tracking IA Awareness training using two separate systems, and the FSO was tracking the SA certification activities using a spreadsheet. The Chief Information Office used the Training Notification and Tracking System, while Manpower, Personnel, and Security used the Corporate Management Information System to track IA

Awareness training. In addition, both of these systems were being replaced by the Washington Headquarters Services Learning Management System and the DISA Online Training System, respectively.

The FSO did not have an effective system to monitor and track SA certification compliance. Instead, the FSO used a spreadsheet to monitor compliance. Currently, the FSO is developing a system called the DoD IA Learning Center. The mission of the DoD IA Learning Center is to establish and maintain the capability to deliver and track IA-related training to the DoD community through a standard web browser coming from a .MIL domain. Specifically, the DoD IA Learning Center will be able to track course information, training registration and completion, and the capability of reporting to multiple databases.

With multiple organizations using multiple systems to track training and certification activities, CS cannot effectively or consistently monitor individual training and certification requirements and completion. As a result, some users may not receive the required IA Awareness training, users may not fully understand their security responsibilities, DISA would have little assurance that all SAs have the proper credentials to effectively manage the systems, and access to sensitive information may be inappropriately granted.

Recommendations and Management Comments

B. We recommend that the Director, Defense Information Systems Agency designate an organization to centrally manage and track all training and certification requirements and completions.

Management Comments. The DISA Chief Information Officer concurred and stated that DISA issued a policy on March 2, 2007, designating the Manpower, Personnel, and Security Directorate as the organization to centrally manage and track all training.

C. Information Assurance

While DISA has made improvements in its overall IA program, additional improvements are still needed in the following areas:

- security documentation,
- audit trails,
- host-based intrusion detection,
- public domain software,
- logical and physical access,
- incident handling,
- configuration management,
- asset management, and
- contingency plans.

CS had not fully implemented Federal, DoD, and DISA policies. Until CS effectively implements an IA program that fully complies with DoD and DISA policy, there is an increased risk to the confidentiality, integrity, and availability of the applications operating in the DECCs.

Information Assurance Requirements

DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, establishes security requirements that apply to the definition, configuration, operations, interconnection, and disposal of DoD information systems. The IA controls developed under these requirements form a management framework for allocating, monitoring, and regulating IA resources that is consistent with Federal guidance provided in Office of Management and Budget (OMB) Circular No. A-130, "Security of Federal Automated Information Resources," November 28, 2000. OMB Circular A-130 requires that agencies implement and maintain an information security program to ensure that adequate security is provided for agency information that is collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

Security Documentation

Security documentation, such as the System Security Authorization Agreement (SSAA), security plans, authority to operate, and Service Level Agreement (SLA), within CS was not consistently developed, approved, maintained, and updated. Without complete, accurate, and current security documentation, CS increases the risk of implementing inadequate security controls, having operating

systems with risks above the accepted level, and failing to address customer requirements.

System Security Authorization Agreement. CS did not consistently develop, maintain, and update the SSAA. The SSAA is a formal agreement between the Designated Approving Authority (DAA), the certifying authority, the IT system user representative, and the program manager. It is used throughout the entire certification and accreditation process and the DAA makes the decision to grant an approval to operate based on the information contained in the SSAA. The certification process is a comprehensive evaluation of the technical and non-technical security features of an information system or site. The accreditation is a formal declaration by the DAA 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.

DECCs Columbus and Oklahoma City did not update their SSAAs to reflect the changes resulting from the CS transformation that occurred during FYs 2004 and 2005. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, requires that the SSAA be modified to reflect new changes when new design requirements emerge or existing requirements are modified. Because of the dynamic nature within the CS environment and the continuous changes in technology, CS management needs to constantly reassess the adequacy and currency of the SSAAs. Without current and complete SSAAs, the CS increases the risk of having inadequate security controls and being noncompliant with DoD policies.

DECCs Columbus, Oklahoma City, and Pacific did not identify site criticality (MAC level) in their SSAAs because the CS did not prepare the SSAAs to include all the DoD Instruction 5200.40 requirements. The Instruction requires that the SSAA identify the criticality and the acceptable risk of the site in meeting the mission responsibilities. CS may not identify and implement proper security controls without the site criticality identified in the SSAAs.

Security Plans. 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. A security plan documents an overview of the information security requirements and describes the security controls in place or planned for meeting those requirements. CS did not consistently develop, maintain, and update the security plans. Specifically, DECC Pacific did not develop an adequate security plan. DECC Pacific used an Information System Security Policy as its security plan which did not contain the required elements of a security plan. In addition, the DECC Columbus security plan did not reflect the current functional description after the CS transformation. OMB Circular A-130 requires that the security plan be updated as necessary. Since CS operates in a dynamic environment and the technology is constantly changing, CS management needs to constantly reassess the adequacy and currency of the security plans. Without current and complete security plans, CS increases the risk of having inadequate security controls and being noncompliant with DoD policies.

Authority to Operate. The DAA did not approve the authority to operate based on timely information. Specifically, DECCs Denver and Jacksonville did not receive an authority to operate in a timely manner; 8 months after their SSAAs were reviewed and signed. This occurred because the DAA did not timely sign the accreditation memo. Outdated, incomplete, and inaccurate information in the SSAA may hinder the DAA decision-making process and increase the likelihood that systems with risks above the accepted level may be approved to operate. Therefore, DISA needs to improve the process to ensure that the accreditation decisions are made in a timely manner.

Service Level Agreements. DoD Instruction 8500.2 requires that outsourced IT services explicitly address Government, service provider, and end user IA roles and responsibilities. CS did not ensure that customers identify relevant IA requirements during the SLA process to protect systems at the required levels. The SLA is the agreement between the customer and CS on the level of support that CS will provide and the expectations of the customer. None of the 45 SLAs:

- identified the MAC level for customer assets and related applications,
- identified the data disposition and sharing requirements, or
- indicated customer acceptance in the form of a signature.

The template used to generate the SLAs did not require the MAC level, data disposition and sharing requirements. In addition, CS did not require their customers to sign the SLA. As a DoD service provider for IT services, CS needs to have a clear understanding of its roles and responsibilities, as well as those responsibilities of the customer for each individual application and system. Without addressing the MAC levels and data disposition and sharing requirements, CS may not implement appropriate system settings in accordance with user requirements, which could lead to a higher level of risk. Without customer signatures, CS cannot execute the agreement to provide customer-requested services or hold customers accountable for expenses incurred.

Audit Trails

CS did not implement effective controls over the creation, review, and security of audit logs. We reported this in our prior year report. Specifically, the audit function was not enabled to create audit logs, audit logs were not reviewed, and audit logs were not properly protected. Audit logs are critical to providing information related to unauthorized and suspicious activities.

UNIX and Windows system auditing was not enabled in accordance with the DoD STIGs. Ten out of 46 UNIX servers failed to capture the required auditable events. The UNIX STIG requires logging all successful and unsuccessful system accesses, unauthorized file access attempts, and system startup and shutdown. Thirteen out of 31 Windows 2000 systems were not configured to audit access to

global system objects and resources. The Windows STIG requires that access events to files, folders, and registry keys be audited.[5]

DECCs Montgomery, Ogden, St. Louis, and San Antonio did not regularly monitor and analyze audit logs in accordance with DoD policy. DoD Instruction 8500.2 requires that audit records from all available sources be regularly reviewed for indications of inappropriate or unusual activities, and that tools be available for the review of audit records and for report generation.

Ten of the 132 systems did not have proper permission settings to protect the audit logs. Specifically, ten Windows devices were improperly configured. DoD Instruction 8500.2 requires that the contents of audit logs be protected against unauthorized access, modification, or deletion. The Windows 2003/XP/2000 Addendum requires that only members of the Auditor Group have full access privileges to Windows audit logs. Full access privileges allow an individual to read, modify, and delete the contents of the audit logs.

Auditing was not enabled and audit logs were not reviewed because information captured by the system logs was voluminous and the sites did not have automated tools to effectively and efficiently review all the logs. Audit log files were not protected because CS personnel were unaware that some permission settings were incorrectly set. Not capturing and reviewing critical system events on a regular basis increases the risk that inappropriate access or activity may not be detected. In addition, unprotected audit logs can be exposed to unauthorized alteration, and exploited to hide unauthorized or suspicious activities.

This condition was previously reported in DoD IG Report Number D-2006-086, "Report on General and Application Controls at the Defense Information Systems Agency, Center for Computing Services," May 18, 2006. We recommended that DISA implement consistent procedures across the entity to create, monitor, review, protect, and maintain CS system audit trails. Specifically, DISA should back up audit trails to a different media, maintain the audit trails for at least 1 year, and configure permission settings correctly. We also recommended that DISA provide a standard set of auditing tools. DISA is currently reviewing various solutions and plans to begin the acquisition of the auditing tool in late FY 2007. While a tool or a set of tools will greatly improve the data analysis portion of the recommendation, DISA will not be able to analyze any breach of its systems if the audit trail does not exist or is not adequately protected. Therefore, the recommendations remain open, and we are not making any new recommendations.

Host-Based Intrusion Detection

CS did not deploy host-based intrusion detection system (HIDS) software on all 19 Windows 2003, 20 of 31 Windows 2000, and 14 of 48 UNIX systems. HIDS monitors a system or applications log files. HIDS responds with an alarm or a

[5] The Windows STIG encompasses The Windows 2003/XP/2000 Addendum and the various National Security Agency Guides to Securing Microsoft Windows.

countermeasure when a user attempts to gain access to unauthorized data, file, or services. DoD Instruction 8500.2 requires that HIDS be deployed for all major applications and for network management assets such as routers, switches, and domain name servers. The Windows STIG requires the Information Assurance Manager (IAM) to ensure DoD servers use HIDS.

This condition was previously reported in DoD IG Report Number D-2006-030, "Report on Diagnostic Testing at the Defense Information Systems Agency, Center for Computing Services," November 30, 2005. We recommended that the Director, CS identify all assets without HIDS and implement HIDS as required. The Director, CS concurred with the finding and stated that HIDS would be implemented DoD-wide once the DoD IA Work Group publishes guidance. According to CS management, DISA awarded a contract to implement a DoD-wide HIDS on March 31, 2006. However, the new DoD-wide HIDS will not be fully implemented until December 2007. Therefore, this recommendation remains open, and we are not making any new recommendations.

Public Domain Software

Thirty-six of 57 computers judgmentally sampled contained unauthorized public domain or personal software. See Table 4 for details. DoD Directive 8500.1 requires that public domain software products and other software products with limited or no warranty, such as those commonly known as freeware or shareware, should only be used in DoD information systems to meet compelling operational requirements. Such products must be thoroughly assessed for risk and accepted for use by the responsible DAA.

Table 4. Unauthorized Software

Location	Devices with Unauthorized Software	Devices Sampled
Columbus	0	3
Mechanicsburg	15	15
Montgomery	1	10
Ogden	11	16
Oklahoma City	4	5
San Antonio	2	5
St. Louis	2	2
Pacific	1	1
Total	**36**	**57**

As part of the CS transformation, CS management began centralizing the local area networks. This centralization was called the Administrative Local Area Network (Admin LAN). One of the goals for the Admin LAN was to standardize

end user desktop and laptop software; therefore, CS was waiting for the implementation of the Admin LAN desktop management capabilities. The use of unauthorized public domain and personal software increases the risk of introducing vulnerabilities to the DoD computing environment.

This condition was previously reported in DoD IG Report Number D-2006-086. We recommended that DISA develop a process to ensure that unapproved public domain software is not installed, to include regular inspection of the workstations. The Director, CS concurred with the finding and stated CS had developed a policy to ensure that public domain software products are not installed on CS systems. This policy includes removing privileged user rights from workstations and monitoring through the implementation of the Admin LAN. However, the monitoring feature within the Admin LAN will not be fully implemented until September 2007. Since we found public domain software was still installed on CS computing devices, this recommendation remains open, and we are not making any new recommendations.

Logical and Physical Access

Controls over the following processes for remote logical access and physical access can be improved:

- remote access authorization,
- remote access two-factor authentication,
- computer facility access authorization,
- computer facility two-factor authentication, and
- physical security policy.

DISA needs adequate logical and physical access controls to prevent unauthorized individuals from gaining access to sensitive information and CS facilities.

Remote Access Authorization. CS did not maintain proper authorization for remote access through a dial-up access. DoD Instruction 8500.2 requires that remote access for privileged functions be discouraged, permitted only for compelling operational needs, and strictly controlled. The Network Infrastructure STIG requires that the IAM develop a policy for secure remote access to the site and that an agreement, signed by the remote user, contains the general security requirements and practices and type of access required by the user. Of 180 users sampled, 17 did not have the appropriate authorization for remote access. Table 5 contains the summary of remote access reviewed by location.

Table 5. Remote Access Agreement		
Location[6]	**Unauthorized Access**	**User Access Agreements Sampled**
Mechanicsburg	4	45
Ogden	6	45
Oklahoma City	7	90
Total	**17**	**180**

The 4 users at DECC Mechanicsburg had unauthorized access to the dial-up service and the 13 users at DECCs Ogden and Oklahoma City did not have remote access agreements on file. This occurred because CS did not fully implement the access authorization process. Without proper access authorization procedures, CS has little assurance over the number of individuals having access to its systems.

Remote Access Two-Factor Authentication. CS did not implement two-factor authentication for remote access. Specifically, DECCs Mechanicsburg, Ogden, and Oklahoma City did not use two-factor authentication for remote dial-up access. The Network Infrastructure STIG requires that the Information Assurance Officer (IAO) or Network Security Officer ensure that all remote users are required to use two-factor authentication to access the network. Two-factor authentication is accomplished by using two of the following: user identification, password, or token. DECCs did not use two-factor authentication for remote logical access because the centralization of remote access, as a feature of the Admin LAN, had not been fully implemented. Without a strong authentication mechanism, CS increases the risk that unauthorized individuals may gain access to sensitive information.

Computer Facility Access Authorization. CS did not maintain proper authorization for computer facility access. From a sample of 566 personnel, 34 individuals did not have the appropriate authorization to access the computer facility. Table 6 contains the summary of computer facility access reviewed by location.

[6] DECC Montgomery does not provide remote access through a remote access server. Therefore, remote access was not tested at DECC Montgomery.

Table 6. Computer Facility Access Agreement		
Location[7]	**Unauthorized Access**	**User Access Agreements Sampled**
Chambersburg	0	33
Columbus	33	45
Dayton	0	11
Huntsville	0	29
Jacksonville	0	25
Mechanicsburg	0	90
Montgomery	0	45
Norfolk	0	19
Oklahoma City	0	55
Ogden	0	45
Pacific	0	45
Rock Island	0	13
San Antonio	0	45
St. Louis	1	45
Warner Robins	0	21
Total	**34**	**566**

DoD Instruction 8500.2 requires that only authorized personnel, with a need-to-know, are granted physical access to computing facilities that process sensitive information or unclassified information. At DECC St. Louis, 1 out of 45 badge access request forms could not be located. At DECC Columbus, 33 out of 45 badge access request forms did not have signatures from the appropriate approving authority. This occurred because CS did not fully implement the access authorization process. Without proper access authorization procedures, CS would not be able to account for all badges issued.

Computer Facility Two-Factor Authentication. Four of 17 DECCs required only one-factor authentication, instead of two-factor authentication. The CS Security Handbook mandates an access control system that requires swiping or presenting of an access card or token and entry of a personal identification number for entry to the computing facility. At DECCs Chambersburg, Pacific, San Antonio, and San Diego, the CS personnel only had to swipe a proximity card to gain access to the computer room. The lack of two-factor authentication increases the risk of unauthorized use of the access card in the event the card is misplaced or stolen.

[7] DECCs Denver and San Diego do not manage access to the computer facility. They were excluded from this test.

Physical Security Policy. DECCs Mechanicsburg, Pacific, and St. Louis did not consistently follow physical security policy. At DECCs Mechanicsburg and Pacific, documentation could not be provided to demonstrate that they performed end-of-day and unannounced security checks within the computer facility. DoD Instruction 8500.2 requires that procedures be implemented to ensure the proper handling and storage of information, such as end-of-day security checks and unannounced security checks within the computing facility. In addition, DECCs St. Louis and Pacific did not have a facility penetration process in place to include periodic, unannounced attempts to penetrate key computing facilities. DoD Instruction 8500.2 requires that a facility penetration testing process be in place. Without periodic physical security checks, CS would not be able to identify and correct physical security weaknesses.

Incident Handling

CS did not consistently complete Reportable Trouble Management System (TMS) Ticket Checklists for 51 of the 242 reportable incidents. Table 7 contains the summary of Reportable TMS Ticket Checklists reviewed by location.

Table 7. Reportable TMS Ticket Checklists

Location[8]	Incomplete Checklists	Checklists Reviewed
Columbus	9	22
Mechanicsburg	6	30
Montgomery	14	90
Ogden	2	30
Oklahoma City	19	65
St. Louis	1	5
Total	**51**	**242**

DISA Computing Services Instruction 360-225-1, "Event Reporting Instruction," December 7, 2004, requires the completion of a Reportable TMS Ticket Checklist for reportable incidents. The reportable incidents are operations incidents that are determined by CS management to have a significant impact on operations. The checklist includes information such as root cause, the troubleshooting performed, the availability of redundant systems, the overall impact on the customer mission, batch processing delays, and the physical location of the equipment or application.

The Reportable TMS Ticket Checklists were not always consistently completed and CS management did not periodically review the Reportable TMS Ticket

[8] DECC San Antonio is not required to enter reportable incidents on production equipment because it only manages development and test systems. Therefore, incident handling was not tested at DECC San Antonio.

Checklists to ensure proper completion. Without understanding the requirements of incident reporting and ensuring checklists are completed, CS has little assurance that the Reportable TMS Ticket Checklists would contain detailed records of the reportable incidents. The lack of detailed records on reportable incidents could prevent CS from effectively identifying incident trends, evaluating incident severity, and enhancing incident handling process.

Configuration Management

Although CS had made significant improvements in its change and configuration management program by issuing the Operational Change and Configuration Management Plan, improvements were still needed over supervisory approvals. We could not obtain evidence of supervisory review for 3 of 175 change requests and 2 of 96 emergency changes, as shown in Table 8. In addition, DECC Pacific did not follow the Operational Change and Configuration Management Plan.

DECC Pacific did not follow the Operational Change and Configuration Management Plan. DECC Pacific tracked changes using a local change request form. This local form did not include elements that would assist the local change control board in determining issues such as customer impact and technical feasibility, as required by the change and configuration plan.

Table 8. Change Approval

Location[9]	Changes Lacked Approval	Changes Tested	Emergency Changes Lacked Approval	Emergency Changes Tested
Columbus	2	16	0	2
Mechanicsburg	1	30	0	24
Montgomery	0	45	0	42
Ogden	0	30	2	12
Oklahoma City	0	35	0	16
St. Louis	0	19	0	0
Total	**3**	**175**	**2**	**96**

These conditions occurred because the DECCs did not consistently follow the CS change management policies and procedures for documenting and approving changes.

Our prior year audit report identified significant weaknesses regarding configuration management. The implementation of the Operational Change and Configuration Management Plan remediated many weaknesses identified in the

[9] Change management was not tested at DECC San Antonio because the DECC only manages development and test systems, not production.

prior year audit. However, CS did not fully enforce the plan. As a result, unauthorized or inappropriate configuration changes could lead to potentially detrimental modifications to customer applications and negatively impact business operations and the CS infrastructure. CS needs to ensure that all changes are properly approved and documented, and that DECC Pacific follow the Operations Change and Configuration Management Plan.

Asset Management

Although CS had effective general and application controls over the Integrated Asset and Configuration Management System (IACMS), CS did not consistently perform the quarterly census audit activities. Specifically, 11 of 16[10] DECCs could not provide evidence of performing the required quarterly audit to reconcile the IACMS data to the actual asset inventory. The IACMS is a web-based application designed and developed by CS to be the central repository of asset and configuration data for all CS-managed IT assets for each processing site. All hardware, software, and applications are required to be listed in the IACMS, and it is the source for all inventory-related data calls. The "DISA Computing Services Operations Operational Change and Configuration Management Plan," March 21, 2006, requires that the DECCs quarterly census audits to compare and reconcile IACMS data to property management and asset accounting records. In addition, the Plan requires that a finding report to be generated within 10 working days following each audit. CS did not consistently perform the quarterly census audit activities because CS did not have detailed procedures to instruct the DECCs on how to conduct the required quarterly census audits. Without periodic validation of asset data, CS would not be able to provide accurate and complete reports in response to CS data calls pertaining to IACMS configuration inventory.

Contingency Plans

While CS made improvements in its contingency plan process, management over contingency plans was not effective. Specifically, the site-specific contingency plans were not comprehensive, and 16 of 17 DECCs did not conduct the annual contingency plan testing.

Site-Specific Contingency Plan. Eleven of 17 DECCs did not have comprehensive site-specific contingency plans. Specifically, DECCs Columbus, Denver, Jacksonville, Ogden, Rock Island, and St. Louis did not identify an alternate process site in their contingency plans. DECCs Chambersburg, Denver, Huntsville, Montgomery, Oklahoma City, Rock Island, San Antonio did not include emergency process priorities in their contingency plans.

[10] IACMS procedures were not tested at DECC Pacific.

DoD Instruction 8500.2 requires that:

- alternate sites be identified that permit the partial restoration of mission- or business-essential functions and

- mission- and business-essential functions are identified for priority restoration planning along with all assets supporting mission or business essential functions.

Periodic Testing. None of the DECCs, with the exception of Mechanicsburg, could provide documentation evidencing the performance of an annual contingency plan test. DoD Instruction 8500.2 requires that the contingency plans be tested annually. This testing would help the DECCs identify deficiencies in the plans, evaluate the viability of the plan, and could assist management in making necessary adjustments.

Our prior year audit report recommendations included: establishing a standard process to review contingency plans to ensure they are comprehensive and complete, and establishing and implementing standard policies and procedures for performing annual comprehensive contingency plan testing. CS made progress by developing site-specific contingency plans and developing a Concept of Operations document, which requires testing and documenting annual comprehensive contingency plans; however, some plans were not comprehensive and did not include emergency processing priorities. As a result, there is an increased risk that critical business operations would be impaired in the event of service interruptions. Therefore, CS needs to ensure that all DECCs have comprehensive site-specific contingency plans to include all the required elements.

Summary

CS still needed to improve its overall IA program. The lack of a comprehensive and integrated IA program could lead to security incidents that could go unprevented and undetected. Specifically, without complete, accurate, and current security documentation, CS increases the risk of operating systems with risks above the accepted level, implementing inadequate security controls, and failing to address customer requirements. Failure to perform the required audit functions increases the likelihood of not detecting inappropriate access or activities. Also, unprotected audit logs are exposed to unauthorized alteration, which could be exploited to hide unauthorized or suspicious activities.

Additionally, the use of unauthorized public domain and personal software increases the risk of introducing vulnerabilities to the DoD computing environment. Also, the lack of a proper access authorization and authentication process and periodic physical security checks increases the risk of unauthorized individuals gaining access to sensitive information and CS facilities.

Further, the lack of complete Reportable TMS Ticket Checklists could prevent CS from effectively identifying incident trends, evaluating incident severity, and

enhancing incident handling process. Without fully implementing the Operational Change and Configuration Management Plan, unauthorized or inappropriate configuration changes could lead to potentially detrimental modifications to customer applications and could negatively impact business operations and the CS infrastructure.

Finally, without developing comprehensive site-specific contingency plans, there is an increased risk that critical business operations would be impaired in the event of service interruptions.

Recommendations, Management Comments, and Audit Response

C.1. We recommend that the Director, Defense Information Systems Agency implement a process to track and monitor the time between the completion of the System Security Authorization Agreement and the accreditation decision to ensure timely decisions.

Management Comment. The DISA Chief Information Officer nonconcurred and stated that the tracking of the SSAA and other certification and accreditation materials will be done through the DISA Certification and Accreditation Database and the Edge IA Portal. The Chief Information Officer suggested that the recommendation be reworded to implement a process to track and monitor the time between the completion of the SSAA and other certification and accreditation material needed for a timely accreditation decision.

Audit Response. Although the DISA Chief Information Officer nonconcurred, the comments are responsive. We agree with the DISA Chief Information Officer on the importance of other certification and accreditation materials and the proposed tracking tool, but we did not reword the recommendation. No further comments are required.

C.2. We recommend that the Director, Center for Computing Services:

a. Implement a process to ensure that the certification and accreditation packages are properly developed, approved, maintained, and updated in accordance with applicable Office of Management and Budget and DoD requirements.

Management Comments. The Director, CS nonconcurred and stated that CS has a process in place to ensure that the certification and accreditation packages are properly developed, approved, maintained, and updated. The Director, CS also indicated that CS will implement the DoD automated tools, as required by the new interim Defense Information Assurance Certification and Accreditation Process, once it is selected by DISA.

Audit Response. Although the Director, CS nonconcurred, the process described to ensure that the certification and accreditation packages are properly developed, approved, maintained, and updated, and the future implementation of the DoD

automated tools satisfies the intent of the recommendation. No further comments are required.

b. Require that the Service Level Agreements address all of the requirements of DoD Instruction 8500.2 to include the identification of criticality and data disposition and sharing requirements.

Management Comments. The Director, CS concurred and stated that CS had updated the SLA format for FY 2007 to include the identification of criticality and data disposition and sharing requirements.

c. Require and verify the customer's formal acceptance of the Service Level Agreements.

Management Comments. The Director, CS concurred and stated that CS had updated the SLA format for FY 2007 requiring each customer to formally accept the SLA.

d. Periodically review all remote access and facility access to ensure that they are authorized and the access request forms are properly documented and maintained.

Management Comments. The Director, CS concurred and stated that the CS Chief of Operations issued a requirement on February 9, 2007, for site directors to review all remote access and facility access to ensure the proper documentation and maintenance of authorization and access request forms.

e. Implement the two-factor authentication mechanism for remote access and physical access across all Defense Enterprise Computing Centers.

Management Comments. The Director, CS concurred and stated that CS is in the process of implementing the two-factor authentication mechanism for remote access and expects to have it fully implemented by December 31, 2007. He indicated that CS requested that the required sites implement the two-factor authentication for physical access.

f. Develop standard procedures for periodic physical security assessments.

Management Comments. The Director, CS concurred and stated that on February 9, 2007, the CS Chief of Operations issued a reminder to all site directors that they are required to have a physical access penetration-testing program in place.

Audit Response. Although the Director, CS concurred and issued a reminder about the requirements, the response did not address procedures on how to conduct the assessments. DISA is in the process of updating many of its IA policies. We will review those policies and DISA compliance next year to determine whether the recommendation can be closed. No further comments are required.

g. Periodically review the Reportable Trouble Management System Ticket Checklists to ensure that Defense Enterprise Computing Center personnel are properly filling out the checklist in accordance with Computing Services Instruction 360-225-1.

Management Comments. The Director, CS concurred and stated that the CS Chief of Operations is in the process of issuing a new Computing Services Incident Response Instruction with a revised checklist. He expects the instruction to be signed and implemented by March 30, 2007.

h. Require that configuration changes be properly approved and documented in accordance with guidelines established by the Operational Change and Configuration Management Plan.

Management Comments. The Director, CS concurred and stated that the CS Chief of Operations issued a reminder to all site directors that changes must be approved and documented in accordance with the Operational Change and Configuration Management Plan.

i. Require Defense Enterprise Computing Center Pacific to follow the Operational Change and Configuration Management Plan.

Management Comments. The Director, CS concurred and stated that DECC Pacific will implement the Operational Change and Configuration Management Plan by March 31, 2007.

j. Establish and implement comprehensive procedures to ensure that the Defense Enterprise Computing Centers perform quarterly census audits and reconciliations of the Integrated Asset and Configuration Management System data.

Management Comments. The Director, CS concurred and stated that the CS Configuration Management Program Office will develop standard operating procedures by March 31, 2007.

k. Periodically review comprehensive site-specific contingency plans to ensure that all required elements are included.

Management Comments. The Director, CS concurred and stated that the CS Enterprise Business Continuity Manager will review all site contingency plans for all required elements by July 31, 2007.

D. Defense Enterprise Computing Center Pacific

The general controls over DECC Pacific were not effective. Specifically, improvements are needed for controls over security documentation, IA Awareness training, account management, system configurations, audit trails, configuration management, public domain software, data backup, fire and emergency response, facility security, and hardware maintenance and disposal. DECC Pacific had not fully implemented DoD and DISA policies that would have mitigated these weaknesses. Until DECC Pacific effectively implements controls that fully comply with DoD and DISA policy, there is an increased risk to the confidentiality, integrity, and availability of the applications operating in DECC Pacific.

General Controls

DECC Pacific was not part of the DISA transformation and was not included in our FY 2005 audit. This audit was the first comprehensive review of the controls at DECC Pacific, and we identified many of the same issues identified during our FY 2005 audit of continental United States locations. These issues included:

- security documentation (discussed in finding D),
- IA Awareness training (discussed in finding B),
- account management,
- system configurations,
- audit trails (discussed in finding D),
- configuration management (discussed in finding D),
- public domain software (discussed in finding D),
- data backup,
- fire and emergency response,
- facility security (discussed in finding D), and
- hardware maintenance and disposal.

Account Management. DECC Pacific did not fully implement account management controls. Block 14 of the access request form, DD Form 2875, was not properly filled out for the two privileged users we selected. Their DD Form 2875s did not identify them as having privileged access. The CS Security Handbook requires that the user's "supervisor must complete Part II, blocks 13 through 20b. The supervisor must identify systems, applications, and privileges." The IAM stated that the process for documenting the two DD Form 2875s as being privileged users had been overlooked. In addition, DECC Pacific did not perform the annual re-validation of privileged user accounts as required by the CS Security Handbook. As a result, there is a risk

that privileged users may be given additional access or have access rights that they no longer need. CS needs to ensure that DECC Pacific adheres to the CS Security Handbook policy on granting system access to privileged users and conducts annual review of privileged user accounts.

System Configurations. DECC Pacific did not consistently follow DoD Instruction 8500.2 policy pertaining to system configurations. We reviewed 12 devices and found, 3 devices were missing both warning banners and screen locks, and 1 device was missing a screen lock setting. DoD Instruction 8500.2 requires a specific DoD logon warning message and workstation screen-lock functionality. We reported this condition previously in DoD IG Report Number D-2006-030, "Report on Diagnostic Testing at the Defense Information Systems Agency, Center for Computing Services," November 30, 2005 We recommended that DISA enforce compliance with the STIGs for configuration and security settings. The Director, CS concurred with the finding and stated that all site IAMs have been re-briefed on the STIGs to include configuration and security settings as part of the SA Certification Program. DISA was in the process of developing this Program during the audit and stated that current SAs will complete the Program by July 31, 2007. The SA Certification Program is expected to include the technical and information assurance requirements of the operating systems and how to implement these requirements within the DISA environment. CS needs to ensure that SAs at DECC Pacific participate in the SA Certification Program.

Additionally, out of 12 devices reviewed, 1 device was not updated with current anti-virus protection. DoD Instruction 8500.2 requires virus protection that includes a capability for automatic updates. DECC Pacific did not have automated tools to push down the virus updates, and updating the virus protection was a labor-intensive process. As a result, non-compliant systems may be exposed to unnecessary risks, such as loss of confidentiality, integrity, or availability of data. CS needs to provide DECC Pacific with a mechanism to automatically receive anti-virus updates.

Data Backup. Controls over the data and program backup procedures were not effective. For example, the DECC Pacific off-site storage agreements were not signed, out of date, and listed former DECC Pacific employees as couriers. In addition, DECC Pacific did not have distance waivers for the off-site storage location being less than the required 25 miles. CS Policy 06-01, "Magnetic Tape Backup and Storage by System Management Center (SMC), Infrastructure Services Center (ISC), and Processing Element (PE) Activities," October 7, 2005, states that a waiver must be signed for distances less than the 25 mile minimum distance between site and off-site location. DECC Pacific needs to have current and signed off-site storage agreements. Additionally, CS needs to provide official documentation accepting the risk of having an off-site storage location less than the required 25 miles away.

DECC Pacific had one iteration of tapes stored at one of the two off-site locations. DISA Computing Services Letter of Instruction 06-01 requires two iterations of backups be maintained at the off-site storage location. In addition, Microsoft Windows backups being sent off-site were incomplete. DoD Instruction 8500.2 requires that data backup be performed daily and recovery media is stored off-site

at a location that affords protection of the data in accordance with its MAC and confidentiality level. DECC Pacific was aware of the situation, but could not identified a cause for the incomplete backup at the time of the audit. As a result, DECC Pacific inappropriately used time and resources by creating incomplete backups and sending them off-site. In the event that a backup needs to be restored, the appropriate backup tapes may not be available for recovery. DECC Pacific needs to have two iterations of backups maintained at the off-site storage location. Additionally, DECC Pacific needs to identify and resolve backup tape creation issues to allow for the creation of complete backup tapes.

Environmental Controls. DECC Pacific did not maintain records proving periodic fire marshal inspection and did not conduct environmental controls training. DoD Instruction 8500.2 requires that computing facilities undergo a periodic fire marshal inspection and deficiencies are promptly resolved and that all employees receive initial and periodic training in the operation of environmental controls. Without proper documentation of fire marshal inspections, DECC Pacific would not be able to promptly resolve deficiencies. In addition, without proper environmental controls training, personnel may not know how to respond in the event of an emergency. DECC Pacific needs to maintain records of fire marshal inspections and provide personnel with environmental controls training and document the training.

Hard Drive Disposal. Controls over hard drive disposals were not effective. DECC Pacific does not maintain a list of all hard drives that have been sanitized, degaussed, or destroyed. The Assistant Secretary of Defense Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001, requires a list of sanitized, degaussed, or destroyed hard drive be maintained by the certifier. Without a record to certify that hard drives have been properly disposed, DECC Pacific would have no assurance that all disposed hard drives have gone through the appropriate precautionary procedures before being released outside DoD. DECC Pacific needs to maintain records of all disposed hard drives to prevent the risk of exposing sensitive DoD information and data.

Recommendations and Management Comments

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

1. Require Defense Enterprise Computing Center Pacific to follow the access authorization and access re-validation procedures for privileged accounts outlined in the Center for Computing Services Security Handbook.

Management Comments. The Director, CS concurred and stated that DECC Pacific completed the re-validation of all privileged access authorizations in accordance with the CS Security Handbook on January 15, 2007.

2. Require Defense Enterprise Computing Center Pacific System Administrators to participate in the System Administrator Certification Program.

Management Comments. The Director, CS concurred and stated that CS now requires all DECC Pacific SAs to participate in the SA Certification Program.

3. Provide Defense Enterprise Computing Center Pacific with a mechanism to receive automatic anti-virus updates.

Management Comments. The Director, CS concurred and stated that DECC Pacific now has a mechanism to receive automatic anti-virus updates.

4. Require that Defense Enterprise Computing Center Pacific have signed and current off-site storage agreements.

Management Comments. The Director, CS concurred and stated that DECC Pacific will have a signed and current off-site storage agreement by March 31, 2007.

5. Provide an official risk acceptance for the Defense Enterprise Computing Center Pacific off-site storage location being less than the minimum required 25 miles.

Management Comments. The Director, CS concurred and stated that the CS Chief of Operations will provide DECC Pacific with a waiver for the off-site storage location being less than the minimum required distance by March 31, 2007.

6. Enforce the Defense Information Systems Agency Computing Services Letter of Instruction 06-01 on Defense Enterprise Computing Center Pacific requiring that two iterations of backups be maintained at the off-site storage location.

Management Comments. The Director, CS concurred and stated that DECC Pacific backup procedures will be compliant with the DISA CS Letter of Instruction 06-01 by April 30, 2007.

7. Assist Defense Enterprise Computing Center Pacific in identifying and resolving backup tape creation issues.

Management Comments. The Director, CS concurred and stated that DECC Pacific will implement proper backup procedures by April 30, 2007.

8. Require Defense Enterprise Computing Center Pacific to adhere to DoD Instruction 8500.2 regarding periodic fire marshal inspections and maintain the inspection records.

Management Comments. The Director, CS concurred and stated that DECC Pacific will have annual fire marshal inspections and maintain the inspection records.

9. Require Defense Enterprise Computing Center Pacific to adhere to DoD Instruction 8500.2 on the training requirements for the operation of environmental controls and maintain the training records.

Management Comments. The Director, CS concurred and stated that DECC Pacific will have its maintenance personnel properly trained by March 31, 2007, and will maintain the training records.

10. Require Defense Enterprise Computing Center Pacific to implement a control to account for all disposed hard drives in accordance with the Assistant Secretary of Defense Memorandum, "Disposition of Unclassified DoD Computer Hard Drives."

Management Comments. The Director, CS concurred and stated that DECC Pacific updated its security standard operating procedures on February 15, 2007, to include the proper procedures for disposing unclassified hard drives in accordance with the Assistant Secretary of Defense Memorandum, "Disposition of Unclassified DoD Computer Hard Drives."

Appendix A. Scope and Methodology

We performed IA and compliance assessment procedures of the DISA CS controls at 17 data processing locations from December 1, 2005, through January 17, 2007. This assessment was performed in accordance with the American Institute of Certified Public Accountants Statement on Auditing Standards 70 and with generally accepted government auditing standards. Specifically, the audit was intended to determine whether DISA (1) general controls over CS are suitably designed and operating effectively; (2) application controls for an internal application system, IACMS, are suitably designed and operating effectively; and (3) CS is in compliance with applicable Federal and DoD IT and IA policies. The scope of this audit was limited to unclassified systems that DISA manages within the DECCs.

The audit methodology used to perform the compliance assessment procedures was developed using the audit methodologies defined by the Federal Information System Controls Audit Manual and the Government Accountability Office (GAO) Financial Audit Manual. The audit program was developed using the CS Security Handbook and the following DoD IA documentation: DoD Directive 8500.1, "Information Assurance," DoD Instruction 8500.2, "Information Assurance Implementation," DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," DoD Manual 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," and DoD STIGs.

SAS 70 Procedures. We assessed the design and operating effectiveness of IT controls specified by DISA management at the following DISA and CS Headquarters locations:

- Arlington, Virginia - Chief Information Office and Manpower, Personnel and Security;
- Chambersburg, Pennsylvania - Business Management Center, Logistics, and FSO;
- Denver, Colorado - CS Headquarters, Business Management Center and Logistics; and
- Falls Church, Virginia - CS Headquarters.

We reviewed the controls at DISA and CS Headquarters locations to obtain an understanding of the centralized functions of the organization. This included obtaining an understanding of the 14 categories on the next page and of the entity-wide policies and procedures for risk assessment, security planning, monitoring, and security management; personnel security and human resource management; and the SLAs process between CS and its user organizations.

We assessed IT controls at the following CS Locations:

Center for Computing Services Locations	
System Management Centers	**Processing Elements**
Mechanicsburg, Pennsylvania	Chambersburg, Pennsylvania
Montgomery, Alabama	Dayton, Ohio
Ogden, Utah	Denver, Colorado
Oklahoma City, Oklahoma	Huntsville, Alabama
Infrastructure Services Centers	Jacksonville, Florida
Columbus, Ohio	Norfolk, Virginia
San Antonio, Texas	Rock Island, Illinois
St. Louis, Missouri	San Diego, California
Defense Enterprise Computing Center	Warner Robins, Georgia
Pearl Harbor, Hawaii	

We conducted a full review at all the System Management Centers, Infrastructure Services Centers, and DECC Pacific. The full review consisted of IT controls in the following 14 categories, as specified by CS.

- security program
- risk assessments,
- site security plans,
- security management,
- personnel policies,
- information resource classification,
- user account management,
- physical access,
- logical access,
- network and telecommunications security,
- incident response,
- access monitoring procedures,
- systems changes to DISA-owned assets, and
- service continuity procedures.

We performed a limited review at all the Processing Elements. The limited review consisted of IT controls in the areas of physical access and service continuity.

Compliance Assessment Procedures. DoD has developed STIGs for a variety of common computer platforms in the DoD environment. We used the DoD STIGs to develop appropriate risk-based audit procedures.

DoD has categorized STIG vulnerabilities into four categories ranging from the most critical (Category I) to least critical (Category IV). Category I and II represent the most significant risk of having an operational impact on CS operations. We tested all Category I and Category II STIG requirements.

We assessed a statistical sample of the CS unclassified systems from May 2006 through July 2006. See Appendix C for statistical sampling details. The compliance assessment procedures included: (1) reviewing the FSO scripts (for those platforms that have such scripts) and validating scripts against the STIGs, (2) running the DISA scripts or performing manual procedures against systems in the selected statistical sample, and (3) evaluating the results against the defined settings in the STIGs. In addition to the scripts, we also reviewed additional reports that were coordinated with FSO and CS such as Computer Associate-Examine for the IBM mainframe systems in the sample. During the audit we encountered a few devices that we could not perform substantive testing. See Appendix C for details.

If a vulnerability was identified through either the script or manual review process, we discussed it with the site IAM and the respective SA. We also requested documentation from CS for the DAA acceptance of the vulnerability, if applicable.

We assessed the DECCs compliance with DITSCAP requirements by reviewing the available SSAA and Certification and Accreditation documentation.

We assessed DECC compliance with DoD Instruction 8500.2 by reviewing documentation supporting the DECC's policies, assignment of responsibilities, and procedures for applying integrated, layered protection of DoD information systems and networks controlled by CS.

Application Controls. We assessed application controls over the IACMS application owned and operated by CS. Specifically, we reviewed the inputs, processes, and outputs of the IACMS application that CS uses to track individual CS computer assets in its computing environment.

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.

Use of Computer-Processed Data. We did not rely on computer-processed data to perform this audit. Rather, we assessed the configuration settings and controls implemented on the devices tested that involved computer-extracted data such as user password settings and services running on the devices.

User of Technical Assistance. The Technical Assessment Directorate of the DoD Office of Inspector General reviewed test plans and audit results.

Additionally, we received assistance from the Quantitative Methods Director of the DoD Office of Inspector General for development of the sampling process.

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.

Appendix B. Prior Coverage

During the last five years, the GAO and the Department of Defense Inspector General (DoD IG) have issued 9 reports discussing the topic of improving DISA investment planning and management controls. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed 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

DoD IG Report No. D-2006-107, "Defense Departmental Reporting System and Related Financial Statement Compilation Process Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004, through March 31, 2005," August 18, 2006

DoD IG Report No. D-2005-086, "Report on General and Application Controls at the Defense Information Systems Agency, Center for Computing Services," May 18, 2006

DoD IG Report No. D-2006-046, "Technical Report on the Defense Property Accountability System," January 27, 2006

DoD IG Report No. D-2006-030, "Report on Diagnostic Testing at the Defense Information Systems Agency, Center for Computing Services," November 30, 2005

DoD IG Report No. D-2006-031, "Report on Penetration Testing at the Defense Information Systems Agency, Center for Computing Services," November 30, 2005

DoD IG Report No. D-2005-105, "Report on Defense Information Systems Agency, Center for Computing Services Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004 through April 30, 2005," September 6, 2005

DoD IG Report No. D-2005-093, "Technical Report on the Standard Finance System," August 17, 2005

DoD IG Report No. D-2005-069, "Audit of the General and Application Controls of the Defense Civilian Pay System," May 13, 2005

Appendix C. Sampling Approach

Overview

The general controls testing required detailed technical analysis of selected security settings and configurations. General controls testing encompassed diagnostic testing, which is the testing of the technical controls implemented in the CS environment. We developed work programs based on the DoD STIGs and DoD Instruction 8500.2. Diagnostic testing consisted of an analysis of data extracted by automated scripts and supplemented by interviews with site SAs. Due to the high number and variety of system devices managed by CS, a statistical sampling approach was employed to select the items to be tested. Upon completion of testing, we summarized exceptions following DoD and DISA criteria, and statistically projected the results to the CS environment.

Sampling Approach and Objective

One of the audit objectives was to determine whether CS general controls were adequately designed and operating effectively. We selected a sample of assets, covering different technologies, to determine the level of compliance with DoD and CS policies. We followed the GAO Financial Audit Manual Section 450 to determine a sample size for diagnostic testing. We used the sampling strategy to obtain an estimated upper limit for the rate of logical information systems controls at risk in the population within 5 percent precision at the 90 percent confidence level for comparison to the GAO Financial Audit Manual; and to obtain an overall estimate of the number of logical information systems controls at risk.

Sampling Design

Sample Frame. The FSO provided an inventory of CS systems extracted from the VMS. The FSO provided an inventory list as of February 14, 2006, that contained 5,767 assets across all CS data centers. We modified the inventory list by eliminating non-applicable assets, DECC Europe assets, and non-CS assets. As a result, the sampling frame contained 4,846 assets. Table C-1 shows the modified sampling frame by group.

Table C-1. Sampling Frame by Group		
Group	**Operating System**	**Assets**
1	Other	1,096
2	IBM Mainframe	127
3	UNIX	1,617
4	Windows	2,006
Total		**4,846**

Sample Size. At 90 percent confidence, the estimated sample size needed to obtain 5 percent precision was 117 items. We imposed a minimum number of 20 items per group, which resulted in a total sample size of 141 items.

During fieldwork, we discovered an additional 22 out-of-scope (such as assets not connected to the network or classified systems) and 18 decommissioned assets. As a result, the original sample of 141 devices decreased to 101 devices available for testing. To maintain a sufficient sample size, we supplemented 40 items to the sample. We selected supplemental assets using the same random seed as the original sample in order to preserve the original selection probabilities and the randomness of the sample. Table C-2 shows the original sample size, the sample available for testing, supplemental items, and the adjusted sample size by group.

Table C-2. Original, Supplemental, and Adjusted Sample Size by Group					
Group	**Operating System**	**Original Sample**	**Original Sample Available for Testing**	**Supplemental Items**	**Adjusted Sample Size**
1	Other	20	8	12	32
2	IBM Mainframe	20	16	4	24
3	UNIX	47	39	8	55
4	Windows	54	38	16	70
Total		**141**	**101**	**40**	**181**

We did not complete testing on all sampled devices. We did not test one mainframe device and one Windows device due to timing constraints. We also discovered that one network device never existed. In addition, we encountered one UNIX device that had a non-configurable operating system. We also did not test three network devices, one UNIX device, and one Windows device due to resource constraints.

Sample Results

Testing Criteria. To determine the non-failure or failure of each device, we used the DISA Computing Services Operations Policy Letter CS 05-09, "Mandatory Information Assurance Guidance," August 31, 2005. For the estimation calculation, we used a total of 181 systems, which included the 22 out-of-scope, 18 decommissioned and 9 not-tested devices. We treated out-of-scope, decommissioned, and not tested items as non-failures. The inclusion of these non-failure items produced a conservative estimate of the percentage of failures. Table C-3 lists the non-failures and failures found within each group.

Table C-3. Sample Evaluation Results

Operating System	Sample Items	Non-Failures*	Failures
Other	32	25	7
IBM Mainframe	24	5	19
UNIX	55	50	5
Windows	70	34	36
Totals	**181**	**114**	**67**

** Non-failures include decommissioned, out-of-scope, and not-tested items.*

Result Interpretations

The estimated percent of logical information systems access controls failures is about 31 percent. The percentage of failures would only apply to the projection of the sample frame of 4,846 assets, as shown in Table C-4. The 90 percent upper confidence bound is about 35 percent.

According to the GAO Financial Audit Manual Section 450, at 90 percent confidence, an upper confidence boundary at less than 5 percent indicates that the auditors can have high reliance on controls; an upper confidence boundary between 5 percent to 10 percent indicates that the auditors can have moderate reliance on controls; and an upper confidence boundary at greater than 10 percent indicates that the auditors can have little or no reliance on controls. Thus, the estimate and the upper confidence boundary exceed the upper tolerable limits, according to GAO Financial Audit Manual Section 450. Based on the sample results, we concluded that the logical information systems access controls are not operating as designed and cannot be relied upon.

Table C-4. Sample Counts by Group									
		Original Counts			Adjusted Sample		Sample Results		
Group	**Operating System**	**Original Population**	**Sample Frame**	**Original Sample**	**Supplemental Items**	**Final Sample**	**Non-Failures**	**Failures**	**Estimated Weights***
1	Other	1,666	1,096	20	12	32	25	7	34.25
2	IBM Mainframe	141	127	20	4	24	5	19	5.29
3	UNIX	1,715	1,617	47	8	55	50	5	29.40
4	Windows	2,245	2,006	54	16	70	34	36	28.66
Total		**5,767**	**4,846**	**141**	**40**	**181**	**114**	**67**	

*The estimation weight is the inverse of the achieved sampling fraction.

Appendix D. STIG Compliance

The CS had ineffective processes for managing computing device configuration in accordance with the DoD STIGs. We identified noncompliant trends in password and account management, system permissions, security settings, mainframe configuration settings, and baseline comparisons. Many of these issues were identified in prior audit reports.

Note: For reporting purpose, we are only including results from the devices that we have performed substantive testing. Therefore, the total number of devices in the body of the report tested will differ from the total number used for statistical projection. See Appendix C for details.

Password and Account Management. CS continued to have issues implementing controls over password policies and account management. Shorter password lengths and infrequently changed passwords increase the likelihood of a successful brute force attack against the account. Also, the use of shared accounts limits the usefulness of audit trails and holding users accountable for their actions. We identified the following issues with CS password and account management.

- Sixteen of 29 Windows 2000, 3 of 19 Windows 2003, and all 4 Windows XP devices were not configured to require password changes for application accounts on an annual basis. The Windows 2003/XP/2000 Addendum (Section 4.4.2) requires application account passwords to be changed on a yearly basis.

- Fifteen of 29 Windows 2000 systems allowed non-administrators to increase quota rights. The Guide to Securing Windows 2000 (Chapter 4) requires that only administrators have the ability to increase the processor quota assigned to a process.

- One of 3 Cisco Routers and 6 of 6 Juniper Routers did not have individual accounts for administrators. The Network STIG (Requirement NET0460) requires that each user have his own account to access the router with a username and password.

- Twenty-three of 46 UNIX devices did not properly configure the account lockout setting. The UNIX STIG (Requirement GEN000460) requires that the account be locked after three consecutive failed logon attempts.

- Two of 19 mainframes did not meet password complexity requirements. The OS/390 and z/OS STIG (Requirement RACF0460) requires that passwords be set to a minimum 8-character mix of letters and numbers.

System Permissions. Permissions to limit access to devices, directories, and files and registry settings were not in compliance with DoD STIGs. System permissions commonly include account privileges to execute processes and access control lists that provide file access permissions. As a result, vulnerabilities

created from incorrectly set permissions could compromise the device and provide users with unauthorized access to configuration settings and data.

Windows Permissions. Eighteen of 29 Windows 2000 and 11 of 19 Windows 2003 systems had incorrect user rights settings that allowed users to act as part of the operating system. The user rights setting defines the user's ability to perform certain system functionality. The Windows STIG (Chapter 5) requires that no one to have the right to act as part of the operating system.

UNIX Permissions. The SAs did not configure 8 of 46 UNIX devices in accordance with the STIG requirement. The UNIX STIG (Requirement G053) requires the SA to ensure that user home directories have initial access permissions set to 700, and never more permissive than 750, unless fully justified and documented by the IAO. A user is assigned a home directory to maintain files for the user's exclusive use. A permission setting of 700 allows read, write, and execute privileges to the owner and no privileges to the user's group or any other user. Permission settings above 750 would allow group read and execution of selected files.

In addition, the SAs did not configure 9 out of 46 UNIX devices with an Umask setting to 077. Umask defines the permissions a file has when the file is initially created on the UNIX device. The UNIX STIG (Requirement G089) requires that the Umask be set to a default value of 077, so only the file owner has read, write, and execute privileges while other users have no privileges.

Network Permissions. Authentication servers were not used to grant administrative access in one of three Cisco Routers and six of six Juniper Routers. The Network STIG (Requirement NET0430) requires the IAO or Network Security Officer to ensure that an authentication server is used to gain administrative access to routers. Authentication servers provide centralized authentication to the routers and controls the authority levels granted to users in them.

Security Settings. Security settings were incorrectly configured for Windows and Network devices. Vulnerabilities created from incorrect security settings could compromise the device and provide users with unauthorized access to configuration settings and data.

Services. Fifteen of 29 Windows 2000 systems did not enable the "Prevent Automatic Updates" setting. Windows STIG (Requirement 5.060) requires that the IAO ensure the "Prevent Automatic Updates" setting is enabled. Settings for services were set incorrectly or not disabled for 24 of 29 Windows 2000, 11 of 19 Windows 2003, and all 4 Windows XP. Windows STIG (Requirement 5.068) requires the IAO and SA to ensure that unnecessary services be removed or disabled. Two of 3 Cisco routers had Proxy ARP enabled. The Network STIG (Requirement NET0780) requires Proxy ARP to be disabled because Proxy ARP would allow a router to extend the network across multiple interfaces. Running unnecessary services, or services not properly secured, could allow a malicious user to exploit vulnerabilities of a service to gain access to the device.

Warning Banners. The SAs did not deploy warning banners on all six Network Juniper routers. The Network STIG (Requirement NET0340) requires that the Network Security Officer ensure the deployment of warning banners on all network devices allowing Secure Shell,[11] telnet,[12] file transfer protocol, or hypertext transfer protocol access. The absence of a warning banner could be construed as an invitation, without restriction, to log on to the device.

Mainframe Configuration Settings. Mainframes at DECCs Mechanicsburg, Ogden and St. Louis were not in compliance with the Mainframe STIG for the following critical mainframe operating system components.

- Fourteen of the 19 mainframes did not have the correct Customer Information Control System configuration. The Customer Information Control System allows programmers to develop application code to perform interactive processing. Section 8.2 of the Mainframe STIG requires that the IAO implement a series of Customer Information Control System permission settings to provide multi-leveled access and resource protection.

- Twelve of the 19 mainframes did not have the correct OS/390 UNIX System Services configuration. The OS/390 UNIX System Services provides a UNIX environment to mainframe users. Section 2.5 of the Mainframe STIG requires a series of configuration settings in order to provide mainframe users with UNIX functions.

- Eight of the 19 mainframes did not have the correct Communication Server configuration. The Communications Server supports secure networking on an enterprise scale. Section 4.4 of the Mainframe STIG requires a series of configuration settings to enhance network security.

Failure to effectively manage the supporting infrastructure increases the risk of an individual gaining unauthorized access to information assets and network resources.

Baseline Comparison. SAs did not follow DoD STIGs for creating, checking, and maintaining system baselines for UNIX and Windows systems. A baseline is an image, record, or backup that contains a snapshot of the system after it has been fully loaded with operating system files, applications, and users. Thus, unauthorized changes may indicate system compromise and a baseline may prevent serious damage by detecting unauthorized changes in a timely manner. The IAO is responsible for verifying the system baseline and the IAM is responsible for setting the overall baseline creation and maintenance policy.

[11] Sometimes known as Secure Socket Shell, it is a UNIX-based command interface and protocol for securely accessing a remote computer.

[12] A utility program and protocol that allows one to connect to another computer on a network. After providing a username and password to login to the remote computer, one can enter commands that will be executed as if entered directly from the remote computer's console.

The following devices did not comply with STIG requirements on baseline comparison.

- Eighteen of 46 UNIX systems did not compare the audit events file to the baseline backup file and follow up on discrepancies. The UNIX STIG (Section 10.1.1) requires that the audit event file be compared against its baseline backup file and for the IAO to investigate any discrepancies.

- Fourteen of 29 Windows 2000 devices and 9 of 19 Windows 2003 devices did not have evidence that system baselines were being created and reviewed by the SA and IAO. The Windows STIG (Requirement 1.024) requires the SA to create, check, and maintain a current system baseline for all servers and critical workstations.

Appendix E. Criteria for Technical Evaluation

All devices from the statistical sample were compared to the following criteria to determine whether each device individually met the criteria to operate in the CS environment.

Connection Approval Process

"Mandatory Information Assurance Guidance, DISA Computing Services Operations Policy Letter 05-09," 31 August 2005.

Mainframe

"SRR Review Procedures OS/390 & z/OS TSS Checklist," Version 5, Release 1.1, January 2006

"SRR Review Procedures OS/390 & z/OS RACF Checklist," Version 5, Release 1.1, January 2006

"SRR Review Procedures OS/390 & z/OS ACF2 Checklist," Version 5, Release 1.1, January 2006

"OS/390 & z/OS Security Technical Implementation Guide," Version 5, Release 1, January 21, 2005

Network

"Network Infrastructure Security Checklist," Version 6, Release 4, December 23, 2005

"Network Infrastructure Security Technical Implementation Guide," Version 6, Release 4, December 16, 2005

"Cisco IOS Router Checklist Procedures Guide," December 2, 2005

"Juniper JUNOS Router Checklist Procedures Guide," December 2, 2005

UNIX

"UNIX Security Technical Implementation Guide," Version 5, Release 1, March 28, 2006

"UNIX Security Checklist," Version 4, Release 4, December 15, 2005

"UNIX Security Technical Implementation Guide," Version 4, Release 4, September 15, 2003

Windows

"Windows 2003/XP/2000 Addendum," Version 5, Release 1, August 29, 2005

"National Security Agency Guide to Securing Microsoft Windows XP," Version 1.1, December 2003

"Microsoft Windows Server 2003 Security Guide," November 23, 2003

"National Security Agency Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set," Version 1.2, December 3, 2002

Appendix F. Acronyms

Admin LAN	Administrative Local Area Network
CS	Center for Computing Services
DAA	Designated Approving Authority
DECC	Defense Enterprise Computing Center
DISA	Defense Information Systems Agency
DITSCAP	Department of Defense Information Technology Security Certifications and Accreditation Process
FSO	Field Security Operations
GAO	Government Accountability Office
HIDS	Host-Based Intrusion Detection System
IA	Information Assurance
IACMS	Integrated Asset and Configuration Management System
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IT	Information Technology
MAC	Mission Assurance Category
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SA	System Administrator
SLA	Service Level Agreement
SRR	Security Readiness Review
SSAA	Systems Security Authorization Agreement
SSO	Systems Support Office
STIG	Security Technical Implementation Guide
TMS	Trouble Management System
VMS	Vulnerability Management System

Appendix G. Report Distribution

Office of the Secretary of Defense

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

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Combatant Commands

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

Other Defense Organizations

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

Non-Defense Federal Organization

Office of Management and Budget
Government Accountability Office

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Oversight and Government Reform
House Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform
House Subcommittee on National Security, and Foreign Affairs, Committee on Oversight and Government Reform

Defense Information Systems Agency, Chief Information Officer Comments

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

IN REPLY REFER TO: Chief, CIO, Strategy & Policy Division (SPI3) MAR 07 2007

MEMORANDUM FOR DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

THROUGH: DEFENSE INFORMATION SYSTEMS AGENCY, OFFICE OF INSPECTOR GENERAL

SUBJECT: Response to The Defense Systems Agency controls over the Center for Computing Services Project# D2006-D00FG-0053.001

In accordance with the established guidelines, attached is SPI 3's response to the report of The Defense Information Systems Agency Controls over the Center for Computing Services, issued 25 January 2007.

1 Enclosure a/s

ALMA J. MILLER, Colonel, USAF
Chief, CIO, Strategy & Policy Division

Quality Information for a Strong Defense

DISA CIO / DAA
Response to DoDIG Report
The Defense Information Systems Agency
Controls over the Center for Computing Services
Project No. D2006-D000FG-0053.001
Dated Jan 25, 2007

Recommendation A Security Technical Implementation Guides

A.2. We recommend that the Director, Defense Information Systems Agency include all vulnerabilities, including those identified during self-assessments, with the appropriate Plan of Action and Milestones in the Vulnerability Management System.

CIO DAA Comments: Concur.

Recommendations B. Training. Page 10.

We recommend that the Director, Defense Information Systems Agency designate an organization to centrally manage and track all training and certification requirements and completions.

CIO DAA Comments: Concur with comments. DISA IA Policy signed 2 Mar 07, para 9.4.6 under roles and responsibilities states that MPS will: "Provide centralized tracking of DISA IA training and certification of the DISA IA workforce within the Agency." Recommend MPS serve as the organization to centrally manage and track all training to better align function with the DISA IA guidance (cross over date: approximately May 07).

Recommendations. Section C1.

C.1. We recommend that the Director, Defense Information Systems Agency implement a process to track and monitor the time between the completion of the System Security Authorization Agreement to the accreditation decision to ensure timely decisions.

CIO DAA Comments: Non Concur with comments. The system security authorization agreement (SSAA) is just one element that is factored into an accreditation decision. Certifier's recommendations, test results, Plans of Action and Milestones (POA&M) for open Category I/II findings are also critical to the process. Taken together, the IA materials provides current configuration of the system/network (SSAA); risk vulnerabilities (test results) and finally risk mitigation strategies (plan of action and milestones). In order to make an informed accreditation decision, all the major materials must be in place prior to coordination. Tracking for this requirement will be done via the DISA Certification and Accreditation Data base and the Edge IA Portal. Recommend

rewording para to: "We recommend that the Director, Defense Information Systems Agency implement a process to track and monitor the time between the completion of the System Security Authorization Agreement and other certification and accreditation materials needed for timely accreditation decisions."

Defense Information Systems Agency, Center for Computing Services Comments

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

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

MAR 0 2 2007

MEMORANDUM FOR DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

THROUGH: DEFENSE INFORMATION SYSTEMS AGENCY, OFFICE OF INSPECTOR GENERAL

SUBJECT: Response to The Defense Information Systems Agency Controls over the Center for Computing Services Project# D2006-D000FG-0053.001

In accordance with established guidelines, attached is Computing Services' response to the report of The Defense Information Systems Agency Controls over the Center for Computing Services, issued 25 January 2007.

1 Enclosure a/s

ALFRED J. RIVERA
Director
Center for Computing Services

CENTER FOR COMPUTING SERVICES RESPONSES TO AUDIT D2006-D000FG-0053.001 CONDUCTED BY DOD-IG 25 JANUARY 2007 REPORT ON THE DEFENSE INFORMATION SYSTEMS AGENCY CONTROLS OVER COMPUTING SERVICES

Condition: Security Technical Implementation Guides (STIGs). (Finding # A)

A.2. We recommend that the Director, Defense Information Systems Agency include all vulnerabilities, including those identified during self-assessments, with the appropriate Plan of Action and Milestone in the Vulnerability Management System.

Center for Computing Services Response: Concur. Center for Computing Services is in the process of implementing the DoD IA tool for IAVA and STIG compliance. The implementation of this project (SCCVI and SCRI) is expected to be completed by 31 December 2007.

Condition: Information Assurance. (Finding # C)

C.2. We recommend that the Director, Center for Computing Services:

a. Implement a process to ensure that the certification and accreditation packages are properly developed, approved, maintained, and updated in accordance with applicable Office of Management and Budget and DoD requirements.

Center for Computing Services Response: Non-concur. Center for Computing Services has a process in place to ensure that certification and accreditation packages are properly developed, approved, maintained, and updated in accordance with applicable Office of Management and Budget and DoD requirements. The Director, Center for Computing Services is briefed on the status of all certification and accreditation packages by the Center for Computing Services Information Assurance Manager on a weekly basis. The new interim Defense Information Assurance Certification and Accreditation Process (DIACAP) instruction requires the implementation of an automated tool. Center for Computing Services will implement the DoD automated solution once it is selected by DISA.

b. Require that the Service Level Agreements address all of the requirements of DoD Instruction 8500.2 to include identification of criticality and data disposition and sharing requirements.

Center for Computing Services Response: Concur. Center for Computing Services has updated the Service Level Agreement (SLA) format for FY 07 to include identification of criticality (MAC level), data disposition and data sharing requirements.

c. Require and verify the customer formal acceptance of the Service Level Agreements.

Center for Computing Services Response: Concur. Center for Computing Services updated the FY07 Service Level Agreement (SLA), requiring customers to formally accept the SLA.

d. Periodically review all remote access and facility access to ensure that they are authorized and the access request forms are properly documented and maintained.

Center for Computing Services Response: Concur. The Chief of Operations disseminated an e-mail on 9 February 2007 requiring site directors to review all remote access and facility access to ensure authorization and access request forms are properly documented and maintained.

e. Implement the two-factor authentication mechanism for remote access and physical access across all Defense Enterprise Computing Centers.

Center for Computing Services Response: Concur. Center for Computing Services is in the process of implementing a solution for the remote access two factor authentication requirements and expects completion of this project by 31 December 2007.

Center for Computing Services has requested local base facilities to implement two factor authentication mechanisms for the computing rooms at the required locations. Center for Computing Services will continue to pursue this issue and will provide updates as projects are completed.

f. Develop standard procedures for periodic physical security assessments.

Center for Computing Services Response: Concur. The Chief of Operations for Computing services disseminated an email to all site directors on 9 February 2007 reminding them of the requirement to have a physical access penetration testing program in place.

g. Periodically review the Reportable Trouble Management System Ticket Checklists to ensure that Defense Enterprise Computing Center personnel are properly filling out the checklist in accordance with Computing Services Instruction 360-225-1.

Center for Computing Services Response: Concur. The Chief of Operations is in the process of issuing a new Computing Services Incident Response Instruction with a revised checklist. The instruction will be signed and implemented by 30 Mar 2007.

h. Require that configuration changes be properly approved and documented in accordance with guidelines established by the Operational Change and Configuration Management Plan.

Center for Computing Services Response: Concur. The Chief of Operation issued an e-mail on 9 February 2007 to all site directors reminding them of the importance of following the Operational Change and Configuration Management plan and ensuring that all changes are properly approved and documented.

i. Require Defense Enterprise Computing Center Pacific to follow the Operational Change and Configuration Management Plan.

Center for Computing Services Response: Concur. Defense Enterprise Computing Center Pacific is implementing Center for Computing Services Operational Change and Configuration Management Plan; progress is tracked by virtue of reports and monthly meetings. The Director, Defense Enterprise Computing Center anticipates compliance by 31 March 2007.

j. Establish and implement comprehensive procedures to ensure that the Defense Enterprise Computing Centers perform quarterly census audit and reconciliation of the Integrated Asset and Configuration Management System data.

Center for Computing Services Response: Concur. Center for Computing Services is addressing this issue with a Standard Operating Procedures (SOP) document being developed by the Computing Services Configuration Management Program Office. The suspense for the SOP is 31 March 2007.

k. Periodically review comprehensive site-specific contingency plans to ensure that all required elements are included.

Center for Computing Services Response: Concur. Center for Computing Services has tasked the Center for Computing Services Enterprise Business Continuity Manager with reviewing all site contingency plans for the required elements in accordance with DoD policies. Center for Computing Services expects the completion of this task by 31 July 2007.

Condition: Defense Enterprise Computing Center Pacific (Finding # D)

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

D.1. Require Defense Enterprise Computing Center Pacific to follow the access authorization and access re-validation procedures for privileged accounts outlined in the Center for Computing Services Security Handbook.

Center for Computing Services Response: Concur. Defense Enterprise Computing Center Pacific revalidated all access authorizations for privileged accounts in accordance with the Center for Computing Services Security Handbook. Action was completed on 15 January 2007.

D.2. Require Defense Enterprise Computing Center Pacific System Administrators to participate in the System Administrator Certification Program.

Center for Computing Services Response: Concur. Center for Computing Services mandates the participation of all Defense Enterprise Computing Center Pacific Services Systems Administrators in the Systems Administrator Certification Program. Defense Enterprise Computing Center Pacific system administrators information has been submitted to the FSO point of contact.

D.3. Provide Defense Enterprise Computing Center Pacific with a mechanism to receive automatic anti-virus updates.

Center for Computing Services Response: Concur. Defense Enterprise Computing Center Pacific has a mechanism to receive automatic anti-virus updates, and the systems identified in the report have been updated to receive automatic anti-virus updates. Action was completed on 15 January 2007.

D.4. Require that Defense Enterprise Computing Center Pacific have signed and current off-site storage agreements.

Center for Computing Services Response: Concur. Defense Enterprise Computing Center Pacific is acquiring a signed and current off site storage agreement. The suspense for this agreement is 31 March 2007.

D.5. Provide an official risk acceptance for Defense Enterprise Computing Center Pacific off-site storage location being less than the minimum required 25 miles.

Center for Computing Services Response: Concur. Defense Enterprise Computing Center Pacific is requesting a waiver for the off site storage location minimum required distance. This action is being tracked by the Operations Chief, Center for Computing Service and the action will be completed by 31 March 2007.

D.6. Enforce the Defense Information Systems Agency Computing Services Letter of Instruction 06-01 on Defense Enterprise Computing Center Pacific requiring two iterations of backups be maintained at the off-site storage location.

Center for Computing Services Response: Concur. Defense Enterprise Computing Center Pacific is in the process of implementing proper back up procedures and expects to be in compliance with the Defense Information Systems Agency Computing Services Letter of Instruction 06-01 by 30 April 2007.

D.7. Assist Defense Enterprise Computing Center Pacific in identifying and resolving backup tape creation issues.

Center for Computing Services Response: Concur. Defense Enterprise Computing Center Pacific is in the process of implementing proper back up procedures. The suspense for compliance is 30 April 2007.

D.8. Require Defense Enterprise Computing Center Pacific to adhere to DoD Instruction 8500.2 regarding periodic fire marshal inspection and maintain the inspection records.

Center for Computing Services Response: Concur. Defense Enterprise Computing Center is requesting that the local fire marshal comply with DoD Instruction requirements, and supply DECC PAC with proper documentation. This action item will be completed annually.

*D.9. Require Defense Enterprise Computing Center Pacific to adhere to DoD Instruction 8500.2 on the training requirements for the operation of environmental controls and maintain the training records.

Center for Computing Services Response: Concur. Defense Enterprise Computing Center Pacific is in the process of training its maintenance personnel on the operation of environmental controls and training records will be maintained. This action will be completed by 31 March 2007.

D.10. Require Defense Enterprise Computing Center Pacific to implement a control to account for all disposed hard drives in accordance with the Assistant Secretary of Defense Memorandum, "Disposition of Unclassified DoD Computer Hard Drives."

Center for Computing Services Response: Concur. Defense Enterprise Computing Center Pacific updated the site Security Standard Operating Procedures (SOP), signed 15 February 2007. The Security SOP includes the proper procedures for disposing unclassified computer hard drives in accordance with the Assistant Secretary of Defense Memorandum, "Disposition of Unclassified DoD Computer Hard Drives."

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)

08 March 2007

MEMORANDUM FOR DISA INSPECTOR GENERAL (IG)

SUBJECT: Response to Draft Report of DISA Computing Services (Project #D2006FG-0053.0001) 25 January 2007

In accordance with established guidelines, enclosed is DISA Field Security Operations response to the subject draft report.

1 Enclosure a/s

/Christine B. McKinney/
MARK S. ORNDORFF
Chief, Field Security
Operations Division

The Defense Information Systems Agency Controls over the Center for Computing Services
Project No. D2006-D000FG-0053.001
Dated 25 January, 2007

Field Security Operations representatives reviewed the draft IG report for Project No. D2006-D000FG-0053.001. Our comments follow:

Finding A Security Technical Implementation Guides

Recommendations.

A.1. We recommend that the Chief, Field Security Operations improve the quality assurance process to ensure that script issues are resolved and inform users of any unresolved issues or noncompliance with Security Technical Implementation Guide requirements.

FSO Response. Concur. Field Security Operations has reviewed this recommendation and concurs with it as written. We have taken proactive measures and implemented the following changes in the security tool development and release process.

The contractor will provide a matrix of requirements for each technology that will be in included in the release.

a. The contractor will develop and provide a specific test plan for each specific update.

b. The test team will be provided a defect report form that they must complete for any update that does not successfully pass the testing.

c. The contractor provides to the government the final results of the testing. This includes all errors that were discovered, those that were fixed and retested, and those that were unresolved.

d. If there are any unresolved errors, FSO will notify the user community with the release notice for the technology or release.

e. Additionally, FSO engaged the Joint Integration Testing Center (JITC) to perform independent testing of the Gold Disk for the remainder of the FY 2007 releases. FSO will expand this effort to include the FSO developed scripts in 2008 based on availability of funding.

Team Members

The Department of Defense Office of the Deputy Inspector General for Auditing, Defense Financial Auditing Service, in conjunction with contract auditors from Ernst & Young, LLP prepared this report. Personnel of the Technical Assessment Directorate and the Quantitative Methods Directorate of the Department of Defense Office of Inspector General also contributed to the report.

Paul J. Granetto
Patricia A. Marsh
Patricia C. Remington
Frank C. Sonsini
Suzette L. Luecke
Anh H. Tran
Michael L. Davitt
Chanda D. Lee-Baynard
Danial J. Olberding
Chi H. Lam
Henry D. Barton
Kandasamy Selvavel
Minh Q. Tran
Ernest Fine
Wen-Tswan Chen
Christopher J. Bitakis
Ann L. Thompson
Erika D. Boyle

Text Here

Inspector General
Department of Defense

Text Here