~~FOR OFFICIAL USE ONLY~~

Report No. D-2011-089 July 22, 2011

Inspector General
United States Department of Defense

Reducing Vulnerabilities at the Defense Information Systems Agency Defense Enterprise Computing Centers

~~FOR OFFICIAL USE ONLY~~

Additional Copies

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

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (703) 604-8932, or by mail:

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

Acronyms and Abbreviations

ATO	Authorization to Operate
CAT	Category
C&A	Certification and Accreditation
CCC	Consolidated Communications Center
CIO	Chief Information Officer
CSD	Computing Services Directorate
DAA	Designated Approving Authority
DECC	Defense Enterprise Computing Center
DISA	Defense Information Systems Agency
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoD OIG	Department of Defense Office of Inspector General
FSO	Field Security Operations
FTP	File Transfer Protocol
IA	Information Assurance
IATO	Interim Authorization to Operate
IAVA	Information Assurance Vulnerability Alert
ID	Identification
IT	Information Technology
MPS	Manpower, Personnel, and Security
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
SA	System Administrator
SP	Special Publication
SRR	Security Readiness Review
STIG	Security Technical Implementation Guide

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

July 22, 2011

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY,
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY,
COMPUTING SERVICES DIRECTORATE

SUBJECT: Reducing Vulnerabilities at the Defense Information Systems Agency Defense Enterprise Computing Centers (Report No. D-2011-089)

We are providing this report for your review and comment. The Defense Information Systems Agency needs to strengthen general controls related to security management, configuration management, and logical access, and comply with the Security Technical Implementation Guides when configuring operating environments. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that recommendations be resolved promptly. The Defense Information Systems Agency comments on Recommendation B.3, D.1.a, D.1.b, D.2.a, and D.2.b were partially responsive. In addition, the Defense Information Systems Agency, Computing Services Directorate, comments on Recommendation A.2 were not responsive. Therefore, we request additional comments on those recommendations by August 22, 2011.

If possible, please send a .pdf file containing your comments to audfmr@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We are unable to accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 601-5868 (DSN 329-5868).

Patricia A. Marsh

Patricia A. Marsh, CPA
Assistant Inspector General
Financial Management and Reporting

Results in Brief: Reducing Vulnerabilities at the Defense Information Systems Agency Defense Enterprise Computing Centers

What We Did

We conducted an information assurance and compliance audit of the Defense Information Systems Agency (DISA) Computing Services Directorate to determine whether general controls complied with applicable Federal and DoD information technology information assurance policies.

What We Found

DISA needs to strengthen general controls related to configuration and security management and logical access, as required by the Security Technical Implementation Guides. Specifically,

- DISA Computing Services Directorate management could not verify that changes to the operating environment were authorized because they did not require the review of system-generated audit logs. This weakness increased the risk that unauthorized system software changes would go undetected and compromise the integrity of customer applications and data.
- DISA did not always maintain effective security management controls for the certification and accreditation process and evidence retention because DISA did not follow DoD requirements. These weaknesses could allow unauthorized modification, disclosure, and loss of DISA customer data.
- The Defense Enterprise Computing Centers in Mechanicsburg, PA, and Ogden, UT did not configure operating environments as required by security policies because the system administrators did not follow configuration requirements. In addition, the Defense Enterprise Computing Center in Ogden did not use documented schedules to ensure security readiness reviews were performed because management did not require them to be documented. These weaknesses could compromise the confidentiality, integrity, and availability of customer applications.
- The Defense Enterprise Computing Centers in Mechanicsburg, PA; Ogden, UT; and St. Louis, MO, did not properly restrict access to privileged accounts. Management at these locations did not apply DoD requirements for limiting access to privileged accounts, stating that employees needed this level of access to perform their job functions. Allowing unrestricted access to privileged accounts could allow personnel to modify operating system files and compromise the integrity of customer applications and data.

What We Recommend

We recommend that the Director, Defense Information Systems Agency, and the Director, DISA, Computing Services Directorate, verify that only authorized changes occur; retain certification and accreditation documentation; configure operating environments as required by Federal and DoD requirements; and restrict access to privileged accounts.

Management Comments and Our Response

DISA agreed with most of the recommendations, with the exception of Recommendations A.2, B.3, D.1.a, D.1.b, D.2.a, and D.2.b. We request additional comments on the final report for these recommendations by August 22, 2011. The other DISA comments were responsive and met the intent of the recommendations. Please see the recommendations table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Director, Defense Information Systems Agency	B.3, D.1.a, D.1.b, D.2.a, and D.2.b	B.1, B.2, B.4, and D.2.c
Director, Defense Information Systems Agency, Computing Services Directorate	A.2	A.1, A.3, A.4, A.5, and C

Please provide comments by August 22, 2011.

Table of Contents

Table of Contents (cont'd)

Introduction

Objective

The overall objective of this information assurance (IA)* and compliance audit was to determine whether general controls[1] established and implemented by the Defense Information Systems Agency (DISA) were designed adequately, operated effectively, and complied with applicable Federal and DoD information technology (IT)* and IA policies. This audit was limited to a review of those controls that are the responsibility of DISA Computing Services Directorate (CSD). Appendix A discusses the audit scope and methodology. In addition, Appendix B lists prior audit coverage, Appendix C discusses performance improvement opportunities, and Appendix D provides a summary of the applicable criteria used during the audit. See Glossary for definitions of technical terms.

Statement on Auditing Standards No. 70

This report supplements our Statement on Auditing Standards No. 70 report, "Defense Information Systems Agency Control Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2009 through April 30, 2010," DoD IG Report No. D-2010-0070, issued on June 30, 2010. The Statement on Auditing Standards No. 70 report evaluated the DISA CSD internal controls at selected System Management Centers, Infrastructure Service Centers, and Consolidated Communications Centers (CCCs). The report determined whether DISA CSD general controls were in place and operating effectively. The report also determined whether DISA CSD complied with DoD and Federal certification and accreditation (C&A) policies. DoD uses the C&A process to identify information security requirements and ensure that systems and major applications adhere to these requirements.

Background

Overview of Operations

DISA is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric[2] solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components, under all conditions of peace and war. DISA is the provider of global net-centric solutions for the nation's war fighters and all those who support them in the defense of the nation. The core services are Acquisition, Enterprise Services, Network Operations, Network Services, Net-Centric Enterprise Services, and Global Information Grid Bandwidth Expansion.

[1] General controls are a subset of an organization's internal controls, which includes the policies and procedures that apply to all or a large segment of an entity's information system to help ensure proper operation.
[2] Net-centric is a continuously evolving community of people, devices, information, and services connected by a communications network to achieve the optimal benefit of resources and better synchronization of events.
* See Glossary

Computing Services Directorate

CSD provides computer processing for combat support functions, including transportation, logistics, maintenance, munitions, engineering, acquisition, finance, medicine, and military personnel readiness. With more than 3,000,000 users, CSD operates more than 1,400 applications in 18 geographically separate facilities, using more than 35 mainframes and 6,000 servers.

CSD supports computing operations on both DISA-owned and customer-owned platforms. Computing services includes computer operations, data* storage, systems administration, security management, capacity management, systems engineering, Web and portal hosting, architectural development, and performance monitoring. DISA facilities operated 24 hours a day and supports both unclassified and classified computing environments. Services are available to the Military Services, Defense agencies, and combatant commands.

The primary headquarters for DISA CSD is at Fort Meade, Maryland. Headquarter elements are in Chambersburg, Pennsylvania; Denver, Colorado; Oklahoma City, Oklahoma; and Pensacola, Florida. The five primary divisions within DISA CSD are Business Service Management, Customer Relationship Management, Operations, Chief Information Officer (CIO), and Service Design and Transition.

Operating Sites

CSD operating sites are called Defense Enterprise Computing Centers (DECCs). DISA divided the DECCs in the continental United States into mission configurations. The following DECCs were included in the scope of this audit.

- **System Management Centers.** The primary responsibilities of each System Management Center are systems management and customer support functions for the mainframe and server computing environments. The System Management Centers we visited were in Mechanicsburg, Pennsylvania; Montgomery, Alabama; and Ogden, Utah.
- **Infrastructure Service Centers.** The Infrastructure Service Centers perform system management for service-based applications and other specialized fielding efforts from CSD customers. The Infrastructure Service Center we visited was in St. Louis, Missouri.
- **Consolidated Communication Centers.** The primary responsibility of a CCC is to manage all classified and unclassified network devices. The CCCs we visited were in Montgomery, Alabama, and Oklahoma City, Oklahoma.

* See Glossary

Information Assurance Support

The following DISA elements have a direct relationship with CSD on IA.

Chief Information Officer

The CIO develops IT policies, performed IT management and strategic planning, develops and evaluates IT investment criteria, and incorporates and disseminates architecture and standards guidance. The CIO also advises on acquisitions for DISA IT and coordinates with the Office of the Secretary of Defense on IT and IT acquisition matters. In addition, the CIO is the Designated Approving Authority (DAA) for DISA-owned and -operated internal IT enclaves* and networks. Finally, the CIO manages the entity-wide programs for Privacy Act and records management, directs the implementation of electronic business and electronic commerce for DISA, and provides support for DoD IA awareness training.

Field Security Operations

Field Security Operations (FSO), the Certifying Authority for the DISA DAA, provides functional Information Assurance Manager services to CSD. The mission of FSO is to provide information systems,* network security products, and direct funding and reimbursable services throughout DoD, including the Military Services, Defense agencies, and combatant commands. FSO provides such support by directing, managing, and protecting critical elements of the Global Information Grid. The FSO:

- develops, implements, and maintains security guidance and processes,
- conducts full scope security reviews,
- provides security training, security training products, and system administrator (SA) certification, and
- implements security architecture and IA tools.

Manpower, Personnel, and Security

The Manpower, Personnel, and Security (MPS) Directorate provides plans, programs, and oversight worldwide in the mission areas of:

- civilian personnel,
- military personnel,
- human resource development,
- organization and manpower program administration,
- payroll,
- travel,
- transportation,
- mail management,
- visual information,
- security, and
- command information.

* See Glossary

The DISA Security Division, within MPS, provides security policy, guidance, and oversight (except for Information Systems Security) to DISA activities worldwide. This division also provides traditional security assistance in information, personnel, physical and special security reviews, and assessments in support of the DISA C&A process.

Control Environment

CSD is responsible for:

- providing core services and meeting the CSD customer expectations through professional and consistent operations services and standard implementation of DoD regulations and policies;
- refining and analyzing operation performance metrics and practices to identify and implement opportunities for improvement in the execution of core operations services; and
- maintaining the integrity* of the security posture of the operations environment.

Review of Internal Controls

DoD Instruction (DoDI) 5010.40, "Managers' Internal Control Program (MICP) Procedures," July 29, 2010, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of controls. We performed an audit of the DISA CSD general controls. General controls include security management, logical and physical access controls, configuration management, and contingency planning. This report describes the weaknesses identified in the DISA CSD general controls environment. We will provide a copy of the report to the senior officials responsible for internal controls at DISA.

* See Glossary

Finding A. Controls for Documenting and Monitoring System Software Changes Need Improvement

DISA CSD's configuration management processes for documenting and monitoring system software changes need improvement. Specifically:

- DISA CSD management did not have the capability to verify system software changes because they did not have a tool that could generate audit logs of the changes. In addition, management did not require the review of system-generated audit logs of changes implemented in the operating environment. These conditions existed because DISA CSD management did not develop policies and procedures that required a review of the audit logs.
- DISA CSD did not consistently maintain documentation of system software changes required by Information Assurance Vulnerability Alerts (IAVAs),[3] including patches, at the DECCs in Mechanicsburg and Ogden. This condition existed because DISA CSD management did not establish procedures for documenting changes as a result of IAVAs.

Inadequate controls over the review of audit logs and documentation of IAVA changes increase the risk that inappropriate and unauthorized changes could be implemented and that required changes might not be implemented. These risks could result in operating system vulnerabilities for customer applications, which would allow internal DISA personnel or external hackers to gain access and modify customer data, affecting the integrity and availability* of their data.

Configuration Management

Configuration management[4] involves the identification and management of security features for all hardware, software, and firmware components of an information system and systematically controls changes to that configuration during the system's life cycle. Establishing controls over the modification of information system components and related documentation helps to ensure that only authorized systems and related program modifications are implemented. Adequate configuration management controls prevent unauthorized changes to information system resources (for example, operating system and hardware configuration) and provide reasonable assurance that systems are configured properly and operating securely, as intended. DISA is responsible for maintaining the system software environment supporting customer applications, including the selection, authorization, testing, approval, and installation of system software releases, patches, and upgrades.

[3] IAVAs identify vendor system software fixes implemented to patch security and other vendor-identified deficiencies.
[4] We did not review configuration management controls over the database or application software on the in-scope servers.
* See Glossary

DISA CSD Could Not Determine Whether Unauthorized Changes Were Made

Although DISA CSD maintained audit logs as required by the Security Technical Implementation Guides (STIGs), DISA CSD management did not have a tool to generate an audit log of system software changes that traced to the change management systems.[5] Additionally, DISA CSD management did not require periodic reviews of system software changes implemented in production operating environments to verify that all changes were authorized. These conditions existed because DISA CSD did not develop policies and procedures that required the review of system-generated audit logs to ensure that only authorized changes occurred. According to DoDI 8500.2, "Information Assurance Implementation," February 6, 2003, a configuration management process should include verification that the process works effectively and prevents changes outside the process. Because DISA CSD did not review audit logs, unauthorized and inappropriate system software changes may not be detected, and the security, integrity, reliability, and availability of customer applications and data could be compromised.

> *… DISA CSD management did not require periodic reviews of system software changes implemented in production operating environments to verify that all changes were authorized.*

The DECCs in Mechanicsburg and Ogden Did Not Have Sufficient Documentation for System Changes

DISA management could not trace system software change requests to corresponding IAVAs. Specifically:

- 59 of 158 IAVAs at DECC Mechanicsburg could not be traced back to an associated change management system record that included approvals and testing evidence.
- 19 of 164 IAVAs at DECC Ogden could not be traced back to an associated change management system record that included approvals and testing evidence. Management also could not provide evidence of a patch installment required by an IAVA.

In addition, DECC Mechanicsburg did not consistently maintain evidence of system software testing. Specifically, testing documentation for 24 of 69 change management system records did not always provide evidence of testing.[6] These conditions existed because DISA management did not establish procedures for documenting system software changes and testing activities. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53,

[5] This population of changes would be used to verify the completeness and accuracy of manually maintained change management records used to document system software change authorizations and other change management activities.

[6] At the DECCs in Ogden and St. Louis, customer organizations assumed responsibility for the completion of system software change testing. As a result, procedures to verify the existence of documentation evidencing the performance of system software change testing were not performed.

"Recommended Security Controls for Federal Information Systems," August 2009, requires DISA to authorize, document, and control changes by testing and reviewing upgrades and modifications to information systems. Without procedures for documenting change management records and testing activities for changes, management cannot ensure that IAVAs were implemented, changes received the proper approvals, or the changes were tested prior to implementation in the production environments. This could leave customer applications susceptible to security breaches that could affect the integrity, reliability, and availability of their data.

DISA CSD should establish stronger controls over system modifications to ensure that only authorized system and program modifications are implemented.

Conclusion

Configuration management deficiencies put DISA CSD at risk of having malicious code introduced into its production environments, compromising the integrity, reliability, and availability of CSD customer applications. Configuration management involves managing security features for hardware and software components of a system, and it controls changes to that configuration during the system's life cycle. Agencies are required to determine minimally acceptable system configuration requirements and ensure compliance with them. Secure configurations minimize vulnerabilities and reduce the risk of network attacks. DISA CSD should establish stronger controls over system modifications to ensure that only authorized system and program modifications are implemented.

Recommendations, Management Comments, and Our Response

A. We recommend that the Director, Defense Information Systems Agency, Computing Services Directorate:

1. Develop a policy requiring the review of system-generated audit logs.

2. Implement a tool that produces system-generated audit logs of system software changes.

3. Compare the audit logs to a list of authorized system software changes to verify that changes to the operating environments are valid.

4. Establish standards outlining requirements for change management documentation, including software testing evidence.

5. Perform periodic audits of the change records to verify compliance with standards at the Defense Enterprise Computing Centers in Mechanicsburg and Ogden.

DISA Comments

The DISA Chief Information Officer (CIO), responding for the DISA CSD Director, agreed with the recommendations and stated that CSD would develop a policy for reviewing system-generated audit logs by the fourth quarter of FY 2011. However, the DISA CIO only partially agreed to implement a tool that produced system-generated audit logs, stating that CSD plans to conduct a business case study to determine whether an audit log tool will satisfy the finding. In addition, CSD plans to perform compliance validations periodically by the fourth quarter of FY 2012, and implement an entity-wide change management system by the second quarter of FY 2012.

Our Response

The comments from the DISA CIO, for the DISA CSD Director, were responsive for Recommendations A.1, A.3, A.4, and A.5, and the actions met the intent of the recommendations. However, comments for Recommendation A.2 were only partially responsive and did not meet the intent of the recommendation. A feasibility study does not provide a viable plan of action on the implementation of the audit log tool. We request additional comments on DISA CSD's plan to implement a tool that produces system-generated audit logs of system software changes.

Finding B. Certification and Accreditation, Evidence Retention, and Background Re-Investigation Weaknesses Identified

DISA did not always maintain effective security management controls for the C&A process, evidence retention, and background re-investigations. Specifically:

- The DECC Ogden enclave operated under an Interim Authorization to Operate (IATO)[7] for 675 days because the enclave had Category (CAT) I and II security weaknesses that needed to be corrected or mitigated;
- The DISA CIO did not grant waivers authorizing the DECCs in Ogden and St. Louis to continue operating under an IATO for more than 360 days. This occurred because the DISA CIO did not follow the requirements of the DoD C&A policy requiring a waiver to continue operating under an IATO for more than 360 days;
- The DISA certifying authority did not consistently retain evidence supporting risk analysis results and recommendations for certification because DISA did not follow C&A requirements for the documentation of validation evidence; and
- MPS did not submit background re-investigation packages to the Office of Personnel Management (OPM) due to an oversight, which prevented them from submitting the re-investigation packages in a timely manner.

Adequate controls over security management decrease the risk that potential security threats could go undetected and allow vulnerabilities to exist in DISA's operating environments. Inadequate controls put customer applications and data at risk to unauthorized access and disclosure.

Security Management

Security management controls, including the security management program, provide the foundation of a security control structure and show senior management's commitment to addressing security risks. The security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and ineffective allocation of security management resources.

[7] An Interim Authorization to Operate is a temporary authorization to operate a DoD information system under the conditions or constraints detailed in the accreditation decision.

DECC Ogden Operated Under an Interim Authorization to Operate for 675 Days

DECC Ogden operated under an IATO for 675 days. Specifically, DECC Ogden operated under five IATOs from October 24, 2008, through September 9, 2010. DECC Ogden was unable to obtain an Authorization to Operate (ATO) because CAT I and II weaknesses existed on the enclave that were not corrected or satisfactorily mitigated. For 10 days during this period, DECC Ogden operated without a valid IATO or ATO.[8] DECC Ogden should not have been operating without a valid ATO or IATO. DISA management stated that the DoD transition to a new type of C&A process in 2008 prevented the site from obtaining an ATO because of the existing CAT I and II weaknesses. After we identified the problem and reported it to DECC Ogden management, the DAA granted the site an ATO on September 10, 2010. Although we requested the information, DISA management did not provide details on what prevented DECC Ogden from resolving the CAT I and II weaknesses. According to the NIST SP 800-53, DISA should authorize the information system for processing before operations begin. Although the DISA CIO stated there was no risk to customer applications, the fact that DECC Ogden operated under an IATO for 675 days means there were risks that could not be mitigated to qualify for an ATO. However, ceasing operations at DECC Ogden would have stopped the hosting of customer applications, causing massive availability issues to the applications that the warfighter depends on for survival. Therefore, based on the serious impact to the warfighter, DISA is unlikely to cease operations as a result of not having a valid ATO or IATO at the DECCs. DISA needs to set the example for its customers by complying with DoD C&A requirements, which would demonstrate DISA's commitment to protecting customer applications and data.

Chief Information Officer Did Not Grant Waivers to the DECCs in Ogden and St. Louis

The DISA CIO did not grant waivers authorizing the enclaves at the DECCs in Ogden and St. Louis to continue operating under an IATO for more than 360 days. This condition occurred because the DISA CIO did not follow the requirements of the DoD C&A policy for granting waivers. The DISA CIO may authorize continued operation under an IATO for systems that have operated for 360 consecutive days, according to DoD C&A requirements, if the DAA certifies that the system is critical to mission accomplishments. The DECCs in Ogden and St. Louis received waivers to operate on consecutive IATOs totaling more the than 360 days, dated May 6, 2010, after we identified the issue. The DECCs in Ogden and St. Louis should not have been operating without waivers. However, DISA provides services critical to the mission of DoD and ceasing operations at DISA would cause debilitating availability issues to systems that the warfighter depends on for survival. Therefore, in the interest of national security, DISA may not be able to cease operations. DISA needs to be an example to their customers by complying with DoD C&A requirements, which would demonstrate DISA's commitment to the protection of critical customer applications and data.

[8] An Authorization to Operate is an authorization granted by a DAA for a DoD information system to process, store, or transmit information. An ATO indicates a DoD information system has adequately implemented all assigned information assurance controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to three years.

Field Security Operations Did Not Retain Supporting Documentation for the Certification and Accreditation Process

The FSO did not consistently retain support for risk analysis results and certification recommendations. Specifically, FSO did not document risk analysis procedures and evidence inspected during the performance of those procedures. In addition, FSO did not retain the results from the risk analysis. The C&A package only included negative results recorded in the Vulnerability Management System. This occurred because DISA did not follow C&A requirements for documenting validation evidence. According to NIST SP 800-37, DISA must document the results of security control assessments, including information necessary to determine the effectiveness of the security controls. Without supporting documentation in the C&A package, there is an increased risk that the DAA could grant an ATO without a full understanding of the enclave risks and vulnerabilities.

FSO management stated DISA was in the process of moving to the Enterprise Mission Assurance Support Service System, which would effectively maintain C&A supporting documentation.

Re-Investigation Packages Were Not Submitted to OPM Within Established Timeframes

MPS did not submit re-investigation packages to OPM. Specifically, for 2 of 40 employee re-investigation packages, MPS did not submit the re-investigation packages to OPM for adjudication within 5 years from the date of completion of the last investigation. These two employees held Top Secret clearances, which required a re-investigation every five years. Although MPS personnel submitted the re-investigation packages after we identified the deficiencies, they admitted that, due to an oversight, they failed to submit the re-investigation packages to OPM. DoD 5200.2-R states that DISA should perform re-investigations five years from the date of completion of the last investigation for employees in critical sensitive positions or employees with a Top Secret clearance. Without timely re-investigations, there is a risk that adverse information that could cause employees to lose their clearance would be unknown to DISA, potentially compromising the confidentiality* of sensitive data.

Conclusion

Security management weaknesses increase the risk that unauthorized loss, modification, or disclosure of DISA customer data for supported financial systems will occur. Security management controls provide a framework and continuing cycles of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls. Clearly assigned security management structure and

If DISA does not establish stronger controls over C&A activities and background re-investigations, the enclave will be vulnerable to malicious activities perpetrated by both unauthorized and authorized individuals.

* See Glossary

responsibilities for security helps to ensure confidentiality, availability, and integrity of an information system and its data. If DISA does not establish stronger controls over C&A activities and background reinvestigations, the enclave will be vulnerable to malicious activities perpetrated by both unauthorized and authorized individuals. Stronger security management controls are necessary to help ensure that DISA makes personnel and enclave ATO decisions with accurate information.

Management Comments on the Finding and Our Response

DISA Comments

The DISA CIO indicated that we did not use the correct reference when providing criteria to support the finding related to the IATOs. Specifically, the DISA CIO stated that DISA does not follow NIST and suggested we revise the criteria from NIST SP 800-53 to the DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process."

Our Response

All Federal agencies are required to comply with NIST policies and procedures. Therefore, our reference to NIST SP 800-53 was correct.

Recommendations, Management Comments, and Our Response

B. We recommend that the Director, Defense Information Systems Agency:

1. Require the certifying authority to review certification and accreditation packages and submit recommendations for certification to the Designated Approving Authority before the current operating status expires.

2. Issue a waiver for mission-critical enclaves operating under consecutive Interim Authorizations to Operate for more than 360 days as required by policy.

3. Retain evidence of all certification activities per DoD and National Institute of Standards and Technology certification and accreditation process requirements.

4. Submit re-investigation packages to the Office of Personnel Management within established timeframes based on the employees' clearance levels as required by policy.

DISA Comments

The DISA CIO, responding for the DISA Director and CSD Director, agreed with Recommendations B.1, B.2, and B.4, stating that DISA now uses the Enterprise Mission Assurance Support Service, which tracks the status of the certification and accreditation packages and logs whether the CIO received certification recommendations before the current operating status expires. In addition, the DISA CIO stated that the Enterprise Mission Assurance Support Service would assist the CIO in tracking weaknesses on systems that operated under an

IATO for more than 360 days. Further, the DISA Director for MPS stated that MPS plans to authorize all CSD Security Managers to access security and personnel adjudication systems to ensure security personnel comply with clearance re-investigation requirements. However, the DISA CIO did not agree with Recommendation B.3 and stated that FSO maintains the risk assessment results supporting the certification recommendation in the Vulnerability Management System.

Our Response

The comments from the DISA CIO, for the DISA Director and CSD Director, for Recommendations B.1, B.2, and B.4 were responsive, and the actions met the intent of the recommendations. However, the comments for Recommendation B.3 were not responsive. Specifically, the DoD C&A policy requires actual results and supporting documentation to be part of the C&A package. This includes artifacts such as output from automated test tools, background materials, or screen shots of system configuration. The package obtained by the DoD OIG did not contain the required supporting documentation. We asked DISA for the documentation that supports the certification recommendation that should have been included in the C&A package. However, as of the date of this report, DISA has not provided the documents to support its position. As a result, we conclude that the finding and recommendation related to the retention of documents that support the certification recommendation was valid and supporting documentation did not exist at the time of the audit. We request additional comments on how DISA plans to resolve this issue.

Finding C. DISA Did Not Always Comply With the Security Technical Implementation Guides

Controls for the operating environments that support customer applications at the DECCs in Mechanicsburg and Ogden were not always configured properly as required by DoD IA requirements and the DISA STIGs. Specifically, some operating environments did not have adequate user account inactivity settings, password settings, and system configurations, which resulted in CAT I vulnerabilities. These conditions existed because the SAs at the DECCs in Mechanicsburg and Ogden did not apply the configuration requirements outlined in STIGs.

In addition, DECC Ogden did not use documented schedules to ensure that Security Readiness Reviews (SRRs) were performed for all UNIX and mainframe assets. This occurred because DECC Ogden management did not have a requirement to document SRR schedules.

These weaknesses created potential system vulnerabilities that could impact the confidentiality, integrity, and availability of customer applications and data.

Information Assurance Compliance

Department of Defense Directive (DoDD) 8500.01E, "Information Assurance," April 23, 2007, established policy and assigned responsibilities for DISA to develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with the National Security Agency. DoDD 8500.01E states that all IA and IA-enabled IT products incorporated into DoD information systems should be configured in accordance with DoD-approved security configuration guidelines. To comply with this directive, FSO developed the STIGs to provide guidelines that ensure an environment meets or exceeds the security requirements of DoD systems operating at Mission Assurance CAT II.[9] We limited our tests of compliance to CAT I and some CAT II[10] potential discrepancy items. We focused our testing approach on CAT I potential discrepancy items because these are vulnerabilities that allow an attacker immediate access into an application, allow super-user access, or bypass a firewall.

DISA CSD Operating Environment Not Always Configured Accurately

DISA CSD did not always configure the operating environments at the DECCs in Mechanicsburg and Ogden according to the DISA STIGs. Specifically,

- Two of 23 Windows servers had non-Auditor user groups with read, write, delete, and execute access rights to the Windows event logs at DECC Mechanicsburg. These access rights allow users to modify or delete system event and log information. DECC Mechanicsburg management stated that the user groups inherited the rights from another

[9] Mission Assurance CAT II systems handle information that is important to the support of deployed or contingency forces. Loss of availability to these systems can only be tolerated for a short time and can cause delay or degradation in providing important support services or commodities that seriously impact mission effectiveness or operational readiness.

[10] CAT II findings are vulnerabilities that provide information that have a high potential of giving system access to an intruder.

group with the same permissions and management did not verify the need for such permissions. The Windows STIG requires that access to the Windows event log be limited to the Auditors group. Without restricting access to event logs, DECC Mechanicsburg increases the risk of masking unauthorized changes to the servers.

- One UNIX server Network Time Protocol Daemon* at DECC Ogden did not point to an authoritative DoD source. This occurred because the SA did not enter the appropriate information when configuring the Network Time Protocol Daemon. The UNIX STIG requires SAs ensure that outside network timeservers are an authoritative DoD source. By not configuring the UNIX server according to STIG requirements, an increased risk exists that the server could be placed on a different time configuration than the hosted applications, possibly disrupting system processes.

- One UNIX server at DECC Ogden did not include the required encryption* within the terms and conditions of the service level agreement with the customer for File Transfer Protocol (FTP) connections outside of the enclave. The UNIX STIG prohibits FTP from outside the enclave into the enclave unless encrypted. According to management at DECC Ogden, the terms and conditions of the service level agreement inadvertently excluded the requirement for encryption. An FTP connection increases the risk of unauthorized individuals viewing customer data since FTP data transmits in clear text.

- On six UNIX servers at DECC Ogden, 125 of 8,469[11] accounts did not lock user accounts after 35 days of inactivity. This occurred because the SAs did not follow up on discrepancies identified by the monthly UNIX STIG SRRs. The UNIX STIG requires accounts to be locked after 35 days of inactivity. Unlocked and inactive accounts increase the risk of unauthorized access to customer applications and their data.

The UNIX STIG requires accounts to be locked after 35 days of inactivity.

- At DECC Mechanicsburg one UNIX user account had a NULL (blank) password. In addition, 1 UNIX system account at DECC Ogden had an easily-guessed password. Management at the DECCs in Mechanicsburg and Ogden stated that these conditions existed because the customers did not apply standard settings when they created the user accounts. The UNIX STIG prohibits the use of easily-guessed and NULL passwords because there is an increased risk that unauthorized users could gain access and make changes to customer applications and data.

These conditions existed because management at the DECCs in Mechanicsburg and Ogden did not ensure the SAs configured the operating environments according to the STIGs. By not

[11] The 125 accounts represent approximately 1.48% of the total population of 8,469 accounts on the 24 UNIX operating environments selected for testing at DECC Ogden. We did not test for accounts inactive for less than 35 days and not configured to lock after 35 days. Therefore, it is possible that more than the 125 accounts were not configured to lock after 35 days.

* See Glossary

configuring DISA CSD operating environments in accordance with STIGs, there is an increased risk that unauthorized individuals could exploit these vulnerabilities to make changes to applications housed on the enclaves or view sensitive customer data.

DECC Mechanicsburg Did Not Run Mainframe Security Readiness Review Scripts Correctly

At DECC Mechanicsburg, the SRR scripts for 1 of 11 logical partitions did not run correctly. Specifically, DECC Mechanicsburg did not generate the SRR results that allowed the SAs to validate configuration settings. This occurred because DECC Mechanicsburg did not configure the datasets appropriately to ensure all automated checks generated the required reports. DISA CSD guidance requires SAs to use automated vulnerability assessment tools, such as SRR scripts and manual vulnerability assessments, to complete Information Assurance Reviews.[12] If SRR results are not reviewed periodically to ensure that all checks are valid, there is the possibility of the vulnerabilities allowing inappropriate access to the mainframe operating environments, which could negatively impact the confidentiality, integrity, and availability of customer applications and their data.

Management Action

During STIG compliance testing, management at the DECCs in Mechanicsburg and Ogden corrected the deficiencies identified for configuring the operating environments in accordance with the STIGs and running the mainframe SRRs. Therefore, we will not make a recommendation on those issues.

Security Readiness Reviews for UNIX and Mainframe Assets

DECC Ogden did not use formal schedules to ensure that SRRs were performed for all UNIX and mainframe assets. This condition existed because DECC Ogden management did not have a requirement to verify that SRRs were performed. DISA's Information Assurance Support Environment online resource stated SRRs were used to test STIG compliance. In addition, the STIGs provide requirements and associated steps system owners should implement to avoid security vulnerabilities. According to NIST SP 800-53, DISA should assess a subset of security controls annually during continuous monitoring, which helps ensure the environment meets or exceeds DoD security requirements. In addition, Office of Management and Budget (OMB) Memorandum M-10-15, dated April 2010, states that management should monitor a subset of controls to ensure the controls are assessed during the authorization cycle. DISA should develop formal schedules to keep track of the controls already assessed and those awaiting assessment. Without formal schedules for SRRs, it may be difficult for DECC Ogden management to track compliant controls to ensure effectiveness of those controls and may be unaware of vulnerabilities that could negatively affect the confidentiality, integrity, and availability of customer applications and their data.

[12] Information Assurance Reviews evaluate the hardware and software configurations of programs, systems, and enclaves to determine whether they comply with DoD IA controls and security requirements.

Recommendations, Management Comments, and Our Response

C. We recommend that the Director, Defense Information Systems Agency, Computing Services Directorate, develop formal schedules documenting the performance of Security Readiness Reviews for UNIX and mainframe assets.

DISA Comments

The DISA CIO, responding for the DISA Director and CSD Director, agreed with the recommendation and stated that Security Readiness Review date schedules have been provided to the DoD OIG and supporting documentation is available upon request.

Our Response

The comments from the DISA CIO, for the DISA Director and CSD Director, were responsive, and the actions met the intent of the recommendation.

Finding D. Logical Access Control Weaknesses Identified

Logical access control weaknesses existed at the DECCs in Mechanicsburg, Ogden, and St. Louis. Specifically, DISA CSD did not restrict access to privileged accounts* based on job responsibilities and the concept of least privilege.* DECC management did not restrict access because management did not apply DoD requirements for limiting access to privileged accounts, stating that granting access to these accounts allowed personnel to perform specific job functions.

In addition,

- DISA CSD did not review audit logs for security events periodically and document the review across all platforms. This occurred because DISA did not have an entity-wide audit logging tool that could analyze the data from audit logs for security abnormalities.
- DECC St. Louis only completed a partial review of privileged accounts during annual revalidations. This occurred because DISA did not have an entity-wide policy that defined the requirements for the annual revalidation of user access.
- DECC St. Louis did not maintain media disposal logs for degaussing* and disposal of sensitive but unclassified tape media. This occurred because management was unaware of a requirement to maintain a media disposal log.

Adequate controls over privileged accounts, audit log reviews, revalidation of system access, and media disposal decreases the risk that users could have unauthorized access to the operating environments, which could compromise the confidentiality, integrity, and availability of the DISA customer applications.

Logical Access

Logical access controls[13] limit or detect inappropriate access to computer resources (data, equipment, and facilities) and protect them from unauthorized modification, loss, and disclosure. Logical access controls require users to authenticate themselves through user identification (ID) and passwords or other identifiers. Authenticated users are then limited to the files and other resources that they can access, and the actions they can execute. Without adequate logical access controls, unauthorized individuals, including outside intruders and former employees, may be able to read and copy sensitive data, and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users can intentionally or unintentionally read, add, delete, or modify data or execute changes that are outside their span of authority.

[13] As part of this audit, the scope included logical access control reviews of the servers' system software environment. This included the operating system and any security software packages used to secure the operating system. Our scope did not include logical access controls over the databases or applications on the servers.
* See Glossary

Privileged Accounts Were Not Restricted

DISA CSD did not restrict access to privileged accounts at the DECCs in Mechanicsburg, Ogden, and St. Louis. Specifically,

Although the Storage Management team did not need complete control over logical access within the mainframe, DECC Mechanicsburg granted 16 members...super-user privileges...

- Although the Storage Management team did not need complete control over logical access within the mainframe, DECC Mechanicsburg granted 16 members of the Storage Management team super-user[14] privileges to the mainframe operating system. DECC Mechanicsburg management stated that the employees needed that level of access to assist customers with emergency issues. DECC Mechanicsburg could have implemented a formal emergency ID process that assigned elevated privileges to emergency IDs to avoid granting super-user access.
- At DECC Ogden, 26 database administrators had ROOT[15] account passwords to the 24 UNIX operating environments selected for testing. DECC Ogden management stated they granted this level of access to allow database administrators to troubleshoot and install quarterly Oracle patches after-hours. Management could have restricted the access to allow personnel to perform limited, elevated functions.
- At DECC St. Louis, one user had full access to mainframe datasets using a privileged account. Although DECC St. Louis management removed the user's access to the privileged account when we identified the issue, management stated they originally granted the user temporary access to this dataset to perform emergency troubleshooting. In addition, users had "write"[16] access privileges to 2 of 45 sensitive mainframe datasets. DECC St. Louis management changed the access to restrict users based on their job responsibilities after we identified the weakness. DECC St. Louis management stated they had not recognized that one of the datasets was sensitive and that the other dataset had an account with inappropriate "write" access.

According to DoDI 8500.2, DISA should limit access to privileged accounts to privileged users such as systems programmers and limit the use of privileged accounts to limited functions. DoDI 8500.2 also states that DISA should only grant individuals who have a valid need-to-know* based on assigned, official Government duties access to restricted information or with special protection measures. The unauthorized use of privileged accounts could allow personnel to modify operating system files and compromise the confidentiality, integrity, and availability of customer applications and data.

[14] A user with super-user access could install changes, create new users, and grant users additional responsibilities.
[15] ROOT is the user name or account that, by default, has access to all commands and files on a UNIX operating system.
[16] "Write" access allows a user to modify the data included within a dataset.
* See Glossary

DISA CSD Did Not Review Audit Logs

DISA CSD personnel did not review audit logs for security events and document the review across all platforms as required by policy. Instead, DISA CSD management stated that they were unable to dedicate resources to perform daily reviews of the significant volume of data generated by the audit logs. As a result, DISA CSD personnel informally reviewed the audit logs and inconsistently documented that review. In addition, DISA CSD could not perform automated reviews of the audit logs because there was no entity-wide tool that could analyze the audit logs for abnormalities. According to DoDI 8500.2, DISA should review audit trail records for indications of inappropriate or unusual activity and report suspected violations. Without audit log reviews, inappropriate security events may go undetected, which could lead to unauthorized access or changes to DISA CSD resources and operating environments.

DECC St. Louis' Annual Privileged User Revalidation Process Needs Improvement

Management at DECC St. Louis did not review the actual access rules configured within the mainframe systems during the annual review of privileged user access. Instead, management only reviewed the access approved on the system authorization form. As a result, DECC St. Louis management could not determine whether a user had access to the system that was not approved on the system authorization forms. This occurred because DISA did not have an entity-wide policy that required an annual review of user accounts using the system-generated listing of privileges. According to NIST SP 800-14, DECC St. Louis should periodically review user account management on a system. In order to fully review logical access privileges, management's review should include verification of the users' access as configured on the system. By not reviewing the actual system access during the revalidation process, management would not be able to identify whether access was properly granted on the system, which the user access forms would not reflect. This increases the risk that users could have unauthorized access to the operating environments and could adversely affect the confidentiality, integrity, and availability of the customer applications and their data.

DECC St. Louis Did Not Maintain Media Disposal Logs

DECC St. Louis did not create a media disposal log that provided evidence of the degaussing and disposal of unclassified magnetic tape media. DECC St. Louis management stated they were unaware of a requirement to maintain a media disposal log for unclassified magnetic tape media. According to NIST SP 800-88, DECC St. Louis should maintain a record of its media sanitization process to include the sanitization date and method, and the final disposition. Inadequate record keeping over media sanitization increases the risk of exposure of sensitive information* to unauthorized individuals.

* See Glossary

Conclusion

The logical access deficiencies identified put DISA CSD at risk that individuals, both authorized and unauthorized, could access or manipulate DISA customer data, which compromises the confidentiality, integrity, and availability of supported customer applications. Logical access controls require users to authenticate themselves using unique identifiers, such as user IDs and passwords. Logical access controls also limit the data authorized users can access and the actions they can execute. Direct access to data files could allow authorized users to make unauthorized changes to the system and its data or introduce malicious code into the system. DISA CSD should improve preventive and detective controls to help ensure that only authorized personnel have access to the operating environments.

Direct access to data files could allow authorized users to make unauthorized changes to the system and its data or introduce malicious code into the system.

Recommendations, Management Comments, and Our Response

D.1. We recommend that the Director, Defense Information Systems Agency:

a. Implement an entity-wide audit logging tool for all operating environments to analyze security event abnormalities. Additionally, develop an entity-wide policy that describes the type of logs to review for security events and the specific methods for documenting the reviews.

b. Develop an entity-wide policy that defines the requirements for the annual revalidation of user access.

DISA Comments

The DISA CIO, responding for the DISA Director, partially agreed to implement an entity-wide audit logging tool and agreed to develop an entity-wide policy requiring annual re-validations of user access. In addition, the DISA CIO provided unsolicited comments, agreeing to implement a tool and develop a policy by the fourth quarter of FY 2011.

Our Response

The comments from the DISA CIO, for the DISA Director, were not responsive and did not meet the intent of the recommendations. Specifically, he stated DISA plans to only assess the capability of audit logging tool within 90 days. The DISA Director also stated that DISA would review the requirements for re-validating user access within 90 days. The responses do not address whether DISA intends to implement an entity-wide audit logging tool or require annual re-validations of user access. We request additional comments on DISA's plan to implement the recommendations.

D.2. We recommend that the Director, Defense Information Systems Agency, Computing Services Directorate:

a. Restrict access to privileged accounts to personnel based on job responsibilities at the Defense Enterprise Computing Centers in Mechanicsburg, Ogden, and St. Louis.

b. Develop procedures at the Defense Enterprise Computing Center in St. Louis to perform an annual revalidation to include a review of users' access configured on the system and formally document the review.

c. Develop procedures that require the Defense Enterprise Computing Center in St. Louis to maintain documentation for sanitizing and disposing of magnetic tape media.

DISA Comments

The DISA CIO, responding for the DISA CSD Director, agreed with the recommendations and stated that CSD restricted access to privileged accounts based on job responsibilities. The DISA CIO, responding for the DISA CSD Director, only stated that the DECC in St. Louis performed the annual revalidation. In addition, he stated that the DECC in St. Louis developed procedures for disposing of magnetic tape media.

Our Response

The comments from the DISA CIO for the DISA CSD Director were responsive for Recommendation D.2.c and met the intent of the recommendation. However, the comments for Recommendations D.2.a and D.2.b were only partially responsive. We were unable to determine whether the DISA CIO, who commented for the DISA CSD Director, agreed or disagreed to restrict access to privileged accounts at the DECCs in Mechanicsburg, Ogden, and St. Louis, and develop procedures at the DECC in St. Louis to perform annual re-validations of users' access. We request the DISA CSD Director to provide additional comments on whether the DECC in St. Louis developed or plans to develop procedures for performing annual re-validations of users' access.

Appendix A. Scope and Methodology

We conducted this performance audit from January 2010 through April 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This report addresses DISA CSD's compliance with Federal and DoD information assurance requirements at the DECCs in Mechanicsburg, Ogden, and St. Louis and the CCCs in Montgomery and Oklahoma City as well as MPS, CIO, and FSO. In addition, we issued a Statement on Auditing Standards No. 70 report on June 30, 2010, that included our assessment on the design and operating effectiveness of the DISA controls. We developed audit procedures to test DISA general computer controls using the methodology in the Government Accountability Office, "Federal Information System Controls Audit Manual," February 2, 2009, and procedures prescribed in DoDI 8500.2.

We interviewed DISA CSD personnel at the DECCs in Mechanicsburg, Ogden, and St. Louis and the CCCs in Montgomery and Oklahoma City. Additionally we interviewed DISA personnel at MPS, CIO, and FSO.

We reviewed logical access control reviews of the DISA servers' system software environment. This review included the operating system and any security software packages used to secure the operating system. We did not test controls covering the databases or applications that reside on the servers. Examples of controls we did not test include, but are not limited to, determining whether:

- changes to databases and applications were authorized and properly tested;
- access to the databases and applications was properly authorized, monitored, and removed in a timely manner; and
- application controls, such as transactional process edits and validations, ensure the completeness and accuracy of application data.

Additionally, we limited our tests of compliance to CAT I and limited CAT II automated checks. We focused our testing on CAT I checks because these vulnerabilities allow an attacker immediate access to applications, super-user access to the operating environments, and the ability to bypass firewalls.

Device Selection Methodology

We obtained a population of applications from DISA CSD that were undergoing audits during FY 2010 and FY 2011, as well as applications DISA wanted to include in the review. We identified the devices[17] that hosted each application. We judgmentally selected the devices to review, giving priority to applications that support financial statement audits for FY 2010. We

[17] Devices included are mainframes, UNIX, and Windows operating environments.

performed STIG compliance testing and SAS 70 general controls testing on the devices selected for review. The total population of devices was 360 and we selected 88 devices to test. The tables below show the breakdown of devices selected in relation to the total population of devices at each location.

Table 1. Mainframe Population and Sample Sizes

Location	Population Size	Sample Size
DECC Mechanicsburg	14	11
DECC Ogden	15	3
DECC St. Louis	14	5

Table 2. UNIX Population and Sample Sizes

Location	Population Size	Sample Size
DECC Mechanicsburg	17	5
DECC Ogden	93	25
DECC St. Louis	0	0

Table 3. Windows Population and Sample Sizes

Location	Population Size	Sample Size
DECC Mechanicsburg	46	23
DECC Ogden	160	16
DECC St. Louis	1	0

Use of Computer-Processed Data

We did not rely on computer-processed data to perform this audit.

Use of Technical Assistance

The DoD OIG Quantitative Methods and Analysis Directorate reviewed the sampling methodology used during the audit. The DoD OIG Technical Assessment Directorate assisted in reviewing audit and test plans and testing compliance with DoD IA and C&A requirements.

Appendix B. Prior Coverage

During the last 5 years, the DoD IG issued 8 reports discussing DISA general controls. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports.

DoD IG Report No. D-2010-070, "Defense Information Systems Agency Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2009 through April 30, 2010," June 30, 2010

DoD IG Report No. D-2009-119, "Defense Civilian Pay System Controls Placed in Operation and Tests of Operating Effectiveness for the Period From October 1, 2008, Through June 30, 2009," September 30, 2009

DoD IG Report No. D-2009-001, "Information Assurance Controls for the Defense Civilian Pay System," October 7, 2008

DoD IG Report No. D-2008-138, "Defense Information Systems Agency Controls over the Center for Computing Services Placed in Operation and Tests of Operating Effectiveness for the Period April 1, 2007, through March 30, 2008," September 30, 2008

DoD IG Report No. D-2007-096, "Information Assurance Controls for the Defense Civilian Pay System," May 14, 2007

DoD IG Report No. D-2007-082, "Defense Information Systems Agency Controls over the Center for Computing Services," April 9, 2007

DoD IG Report No. D-2007-022, "Defense Information Systems Agency Controls of the Center for Computing Services Placed in Operation and Tests of Operating Effectiveness for the Period December 1, 2005, through July 31, 2006," November 15, 2006

DoD IG Report No. D-2006-074, "Technical Report on the Defense Civilian Pay System General and Application Controls," April 12, 2006

Appendix C. Performance Improvement Opportunities

We identified the following performance improvement opportunities. Implementation of these improvement opportunities could strengthen configuration and physical access controls at DISA CSD locations. These opportunities are suggestions and we will not issue recommendations.

CSD Had Several Different Configuration Management Systems

The DECCs in Mechanicsburg, Ogden, and St. Louis and the CCCs in Montgomery and Oklahoma City used multiple configuration management systems to track configuration changes from request to implementation. Additionally, DECC Ogden used two different configuration management systems. This occurred because DISA management did not require the DECCs and CCCs to standardize their configuration management systems. According to DoDI 8500.2, DISA CSD is required to ensure that DoD information systems* operate effectively and provide appropriate confidentiality, integrity, and availability. By not implementing a standardized configuration management process that uses one configuration management system, there is increased risk that vulnerabilities identified and corrected at one site may not be identified or corrected using the same method at another site. Although there are no requirements to standardize the configuration management systems, we suggest DISA CSD management standardize configuration management systems. This would improve DISA CSD management's ability to monitor, evaluate, and manage the configuration process.

Monitoring the Adjudication Status of Interim Security Clearances for Contractors

DECC Ogden did not implement a process to regularly monitor the adjudication status of interim security clearances for contractors in the Joint Personnel Adjudication System. If regular reviews of the adjudication status of interim security clearances for contractors is not implemented, a contractor with a negative adjudication could retain privileged access. This could allow contractor personnel to modify operating system files, which would negatively impact the confidentiality, integrity, and availability of customer applications and their data. Although there are no requirements for implementing a process to monitor the adjudication status of contractors, we suggest DECC Ogden implement a monthly monitoring process to inspect Joint Personnel Adjudication System records of contractors that have interim clearances.

* See Glossary

Site-Level Physical Access Revalidation Policy Needed at DECC St. Louis

DECC St. Louis management did not develop a site-level policy for physical access revalidations. If policies are not documented, the risk is increased that DECC personnel will not follow established, but informal, procedures when performing physical access reviews. This could ultimately allow unauthorized individuals access to the facilities that house sensitive customer data. Although there are no formal requirements to develop a site-level revalidation policy, we suggest DECC St. Louis develop procedures for their annual revalidation of physical access process.

Informal Contractor Tracking Procedures

DISA CSD did not implement entity-wide procedures for Contracting Officer Representatives to track contractor in- and out-processing activities. Without entity-wide procedures, there is increased risk that contractor personnel could retain physical and logical access, which could negatively impact the confidentiality, integrity, and availability of customer applications and their data. Although there are no formal requirements to track the in- and out-processing activities of contractors, we suggest DISA CSD management implement entity-wide procedures for tracking contractors.

Appendix D. Federal and DoD Guidance

We used the guidance below related to information and system security to execute the DISA CSD audit.

Office of Management and Budget

OMB Memorandum M-10-15, "FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," April 21, 2010, provides instructions for meeting an agency's FY 2010 reporting requirements under the Federal Information Security Management Act of 2002. These instructions include frequently asked questions on C&A of information systems.

National Institute of Standards and Technology

NIST developed SP 800-53, "Recommended Security Controls for Federal Information Systems," August 2009, to further its statutory responsibilities under the Federal Information Security Management Act of 2002. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal agency operations and assets except national security systems. This guideline is consistent with the requirements of the OMB Circular A-130, "Management of Federal Information Resources," Section 8b (3), "Securing Agency Information Systems," as analyzed in "Appendix IV: Analysis of Key Sections of the Circular." Appendix III of the Circular, "Security of Federal Automated Information Resources," provides supplemental information.

NIST SP 800-37, "Guide for the Security and Accreditation of Federal Information Systems," May 2004, provides guidelines for the C&A of information systems supporting the Federal Government by:

- enabling more consistent, comparable, and repeatable assessments of security controls in Federal information systems;
- promoting a better understanding of agency-related mission risks resulting from the operation of information systems; and
- creating more complete, reliable, and trustworthy information for authorizing officials, to facilitate more informed security accreditation decisions.

NIST SP 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," September 1996, provides a baseline that organizations can use to establish and review their IT security programs. The document gives a foundation that organizations can reference when conducting multi-organizational businesses as well as internal businesses. Management, internal auditors, users, system developers, and security practitioners can use this guideline to gain an understanding of the basic security requirements most IT systems should contain.

NIST SP 800-88, "Guidelines for Media Sanitation," September 2006, will assist organizations in implementing a media sanitation program with proper and applicable techniques and controls for sanitation and disposal decisions, considering the security categorization of the associated system's confidentiality.

DoD Guidance

DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process," November 28, 2007, establishes a C&A process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD ISs, including core enterprise services- and Web services-based software systems and applications.

DoDD 8500.01E, "Information Assurance," April 23, 2007, established policy and assigned responsibilities for DISA to develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with the National Security Agency. DoDD 8500.01E states that all IA and IA-enabled IT products incorporated into DoD information systems should be configured in accordance with DoD-approved security configuration guidelines.

DoDI 8500.2, "Information Assurance Implementation," February 6, 2003, implements the policies outlined in DoDD 8500.01E by establishing baseline requirements for controls related to IA, emphasizing implementation of need-to-know access controls, and requiring the implementation of certain encryption controls. DoDD 8500.01E defines IA as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.* These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. The instruction requires DoD to assess information systems regularly for IA vulnerabilities and implement appropriate IA solutions to eliminate or otherwise mitigate identified vulnerabilities.

DoD 5200.2-R, "Personnel Security Program," January 1987, implements the DoD Personnel Security Program. It establishes policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces, DoD civilian, consultant, and contractor personnel and of granting such persons access to classified information are clearly consistent with the interests of national security.

The DISA STIGs are the configuration standards for DoD IA and IA-enabled devices and systems. A Security Checklist (sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration) is essentially a document that contains instructions or procedures to verify compliance to a baseline level of security. SRRs test products for STIG compliance. SRRs are available for all operating systems and databases that have STIGs and Web servers using Internet information services. The SRRs are unlicensed tools developed by the FSO, and the use of these tools on products is completely at the user's own risk. For example, the z/OS

* See Glossary

Access Control Facility STIG, Version 6, April 24, 2009, is used to secure mainframes running this security software and operating system. During the course of our review, we referenced the following STIGs:

- Network Infrastructure STIG, Version 7, Release 1, October 25, 2007;
- S/390 Logical Partition STIG, Version 2, Release 2, March 4, 2005;
- SRR Review Procedures MVS Logical Partition, Version 2, Release 1.4, April 2006;
- UNIX STIG, Version 5, Release 1, March 28, 2006;
- Windows 2003/XP/2000/Vista Addendum, Version 6, Release 1, May 21, 2007;
- Windows 2000 Security Checklist, Version 6, Release 1.16, February 26, 2010;
- Windows 2003 STIG Overview, Version 6, Release 1.16, February 26, 2010;
- z/OS Access Control Facility STIG, Version 6, Release 2, December 25, 2009;
- z/OS Resource Access Control Facility STIG, Version 6, Release 2, December 25, 2009; and
- z/OS TSS STIG, Version 6, Release 2, December 25, 2009.

Glossary

Availability. Timely, reliable access to data and information services for authorized users.

Confidentiality. Assurance that information is not disclosed to unauthorized entities or processes.

Data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities, to which meaning is or might be assigned.

Degaussing. Exposing magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media.

DoD Information System. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

Enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personal and physical security. Enclaves always assume the highest mission assurance category and security classification of the automated information system applications or outsourced IT-based processes they support, and they derive their security needs from those systems. They provide standard information assurance capabilities, such as boundary defense, incident detection and response, and key management, and deliver common applications, such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

Encryption. Algorithmic schemes that encode plain text into nonreadable form to provide privacy.

Information Assurance. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD component. Equipment is used by a DoD component either directly or by its contractor. The

term “information technology” includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Integrity. Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

Least Privilege. The principle that users’ are limited to access only the information and resources that are necessary to perform their job responsibilities.

Need-to-Know. Necessity for access to, or knowledge or possession of, specific official information required to carry out official duties.

Network Time Protocol Daemon. Network Time Protocol Daemon is a program that runs in the background of an operating system that synchronizes the clocks of computer systems over a data network.

Nonrepudiation. Assurance that the sender of data receives proof of delivery and the recipient receives proof of the sender's identity, so neither can later deny having processed the data.

Privileged Accounts. Used to modify system data or files, perform special application and database functions, or create user accounts.

Sensitive Information. Information for which the loss, misuse, unauthorized access to, or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled, but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Examples of sensitive information include, but are not limited to, information in DoD payroll, finance, logistics, and personnel management systems.

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FT. MEADE, MARYLAND, 20755-0549

IN REPLY REFER TO: Chief Information Officer (CIO)

18 May 2011

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

THROUGH: DEFENSE INFORMATION SYSTEMS AGENCY, OFFICE OF INSPECTOR GENERAL

SUBJECT: Defense Information Systems Agency response to the report "Reducing Vulnerabilities at the Defense Information Systems Agency Defense Enterprise Computing Centers" dated 18 April 2011.

In accordance with established guidelines, attached is the response to the Reducing Vulnerabilities at the DISA Defense Enterprise Computing Centers report from Computing Services Directorate, Chief Information Officer, and Field Security Operations.

3 Enclosures a/s

DoD OIG: (b) (6)

Chief Information Officer

DoD IG DRAFT REPORT
Project #D2010-D000FG-0096.001
Reducing Vulnerabilities at the
Defense Information Systems Agency
Defense Enterprise Computing Centers

COMPUTING SERVICES DIRECTORATE (CSD) COMMENTS TO RECOMMENDATIONS:

RECOMMENDATION A.1: Develop a policy requiring the review of system-generated audit logs.

DISA CSD RESPONSE: Concur. CSD is developing a policy for reviewing of system generated audit logs. The ECD is FY 2011 Q4.

RECOMMENDATION A.2: Implement a tool that produces system-generated audit logs of system software changes.

DISA CSD RESPONSE: Concur. CSD is currently in the process of a business case feasibility study to determine the likelihood that a proposed product and/or development will alleviate this finding.

RECOMMENDATION A.3: Compare audit logs to a list of authorized system software changes to verify the changes to the operating environments are valid.

DISA CSD RESPONSE: Concur. Recommendation A.3 has a shared dependency with Recommendation A.1 and A.2. The Compliance, Verification and Assistance Branch will be performing periodic compliance validation.

RECOMMENDATION A.4: Establish standards outlining requirements for change management documentation, including software testing evidence.

DISA CSD RESPONSE: Concur. CSD is in the process of implementing an enterprise-wide change management system. The ECD is FY 2012 Q2.

RECOMMENDATION A.5: Perform periodic audits of the change records to verify compliance with standards at the Defense Enterprise Computing Centers in Mechanicsburg and Ogden.

DISA CSD RESPONSE: Concur. The Compliance, Verification and Assistance Branch will be performing periodic compliance validation. The ECD is FY 2012 Q4.

RECOMMENDATION C: We recommend that the Director, Defense Information Systems Agency, Computing Services Directorate, develop formal schedules documenting the performance of Security Readiness Reviews for UNIX and mainframe assets.

DISA CSD RESPONSE: Concur. The Security Readiness Review (SRR) date schedules have been provided to this year's SAS70 team. Support documentations are available upon request.

RECOMMENDATION D.1.a: Implement an entity-wide audit logging tool for all operating environments to analyze security event abnormalities. Additionally, develop an entity-wide policy that describes the type of logs to review for security events and the specific methods for documenting the reviews.

DISA CSD RESPONSE: Concur. CSD has completed the Concept of Operation (CONOPS). Supporting documentation is available upon request. The audit logging tool ECD is FY 2011 Q4.

RECOMMENDATION D.1.b: Develop an entity-wide policy that defines the requirements for the annual revalidation of user access.

DISA CSD RESPONSE: Concur. CSD has started the development of the entity-wide policy for the annual revalidation for users privilege access. The ECD is FY 2011 Q4.

RECOMMENDATION D.2.a: Restrict access to privileged accounts to personnel based on job responsibilities at the Defense Enterprise Computing Centers in Mechanicsburg, Ogden, and St. Louis.

DISA CSD RESPONSE: Concur. CSD has delineated and restricted access to privileged accounts based on job responsibilities. Supporting document is available upon request.

RECOMMENDATION D.2.b: Develop procedures at the Defense Enterprise Computing Center in St. Louis to perform an annual revalidation to include a review of users' access configured on the system and formally document the review.

DISA CSD RESPONSE: Concur. STL has performed the annual validation of user access. Support document is available upon request.

RECOMMENDATION D.2.c: Develop procedures that require the Defense Enterprise Computing Center in St. Louis to maintain documentation for sanitizing and disposing of magnetic tape media.

DISA CSD RESPONSE: Concur. STL has developed procedures for disposing of media. Support document is available upon request.

DODIG DRAFT REPORT
Project No. D2010-D000FG-0096.001
Reducing Vulnerabilities at the
Defense Information Systems Agency
Defense Enterprise Computing Centers

DEFENSE INFORMATION SYSTEMS AGENCY COMMENTS TO RECOMMENDATIONS:

RECOMMENDATION #B.1 Require the certifying authority to review certification and accreditation packages and submit recommendations for certification to the Designated Approving Authority before the current operating status expires.

DISA's Response: Concur. As of January 2011, DISA has moved to the Enterprise Mission Assurance Support Service (eMASS) which would effectively track status of C&A packages. DISA CIO will log any discrepancies if we do not receive certification recommendations before the current operating status expires.

RECOMMENDATION #B.2 Issue a waiver for mission-critical enclaves operating under consecutive Interim Authorizations to Operate for more than 360 days as required by policy.

DISA's Response: Concur. With eMASS and VMS, DISA CIO will be able to track CAT II weaknesses that have operated for 360 consecutive days and the DAA will certify in writing or through DoD PKI-certified digital signature that continued system operation is critical to mission accomplishment. A Standard Operating Procedure will be developed and included in the DISA Playbook on the DIACAP Knowledge Service. A copy of the authorization to continue system operation with supporting rationale shall be provided to the DoD SIAO.

RECOMMENDATION #D.1.a. Implement an entity-wide audit logging tool for all operating environments to analyze security event abnormalities. Additionally, develop an entity-wide policy that describes the type of logs to review for security events and the specific methods for documenting the reviews.

DISA's Response: Partially concur. DISA will review and assess the capability of an entity-wide audit logging tool within 90 days. Furthermore, DISA will need to determine the types of logs to be reviewed for security events and the specific methods for documenting the reviews within 90 days.

RECOMMENDATION #D.1.b. Develop an entity-wide policy that defines the requirements for the annual revalidation of user access.

DISA's Response: Concur with comment. DISA will review the requirements for annual revalidation of user access and address the need for an entity-wide policy within 90 days.

DISA comments on other recommendations and general comments:

On page 9, under "DECC Ogden Operated Under an Interim Authorization to Operate for 675 days", statement "According to the NIST SP 800-53...." uses the wrong reference. DISA follows DoDI 8510.01, not NIST SP 800-53. Reword as follows: "According to DoDI 8510.01, para 5.8.3, DISA shall comply with all accreditation decisions, including denial of authorization to operate (DATO), and enforce authorization termination dates (ATD).

On page 26, under DoD Guidance, there is no reference to DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)" November 28, 2007. DIACAP establishes a C&A process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DoD ISs.

DoD IG DRAFT REPORT
Project #D2010-D000FG-0096.001
Reducing Vulnerabilities at the
Defense Information Systems Agency
Defense Enterprise Computing Centers

FIELD SECURITY OPERATIONS (FSO) COMMENTS TO RECOMMENDATIONS:

RECOMMENDATION #B.3 Retain evidence of all certification activities per DoD and National Institute of Standards and Technology certification and accreditation process requirements.

DISA's Response: Non-Concur. FSO consistently maintains supporting risk assessment results to support Certification Recommendations. The results of the certification testing for the OS, applications, networks and physical environment are loaded into the Vulnerability Management System (VMS). The results of the DoDI 8500-2 IA Controls are also loaded into the VMS. A full assessment of these results are conducted by the FSO Security Control Assessors and a determination of risk is made through two levels of management at FSO. The Certification Recommendation, including the results of the risk assessment is signed by the Certifying Authority (CA) and forwarded to the DISA DAA for a determination of Authority to Operate (ATO). These signed memoranda for each DISA Activity is maintained by the DISA FSO and the DISA DAA.

FSO does follow the Certification and Accreditation guidance of DoD Instruction 8510, DIACAP and the NIST Special Publication 800-37. These documents were developed and issued by DoD and NIST as recommendations and guidance. The application of the Risk Management Framework described in NIST SP 800-37 is flexible, allowing organizations to effectively accomplish the intent of the specific tasks within their respective organizational structures to best manage information system-related security risks. It is our contention that the Certification process followed by FSO meets both the spirit and intent of NIST SP 800-37, dated February 2010.

~~FOR OFFICIAL USE ONLY~~

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

19 MAY 2011

IN REPLY REFER TO: Manpower, Personnel, and Security (MPS)

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

Subject: Technical SAS 70 Draft Report

1. The Defense Information Systems Agency (DISA) has reviewed the draft report referenced above and provides their comments as attached. These comments are meant to provide clarity over finding B. We thank the DOD IG audit team for their opportunity to participate in this audit and hope we provided useful information to complete this task.

2. We look forward to continuing to work with you and your staff in the future. [redacted] Please do not hesitate to contact them should you need to discuss this further.

DoD OIG: (b) (6)
[redacted]

1 Enclosure
DISA Response

Director for Manpower,
Personnel and Security

DoD IG REPORT
Project Number *D2010-D000FG-0096.001*

Reducing Vulnerabilities at the Defense Information Systems Agency Defense Enterprise Computing Centers

DEFENSE INFORMATION SYSTEMS AGENCY COMMENTS TO FINDINGS:

Finding B…Certification and Accreditation, Evidence Retention, and Background Re-Investigation Weaknesses Identified.

3. **DISA's response:** Concur with comment. MPS6 reviewed the finding and determined re-investigation packages were not submitted to OPM within established timeframes and concurs this did occur. Two of the candidate samples identified were not submitted prior to the anniversary date of their background investigation. MPS6 has re-enforced the requirements to the respective specialists. Further, MPS6 has authorized CSD Security Managers at all locations access to the Corporate Management Information System (CMIS) security section as well as the Joint Personnel Adjudication Systems (JPAS) which allows on site management of the identification of security clearance re-investigation requirements to ensure future oversights don't occur.

~~FOR OFFICIAL USE ONLY~~

Inspector General
Department of Defense

~~FOR OFFICIAL USE ONLY~~