U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Subject:

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S INTEGRATED SECURITY MANAGEMENT SYSTEM FY 2009

Report No. 4A-CI-00-09-052

Date: August 10, 2009

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S INTEGRATED SECURITY MANAGEMENT SYSTEM FY 2009

WASHINGTON, D.C.

Report No. 4A-CI-00-09-052

Date: August 10, 2009

Michael R. Esser
Assistant Inspector General
for Audits

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S INTEGRATED SECURITY MANAGEMENT SYSTEM FY 2009

WASHINGTON, D.C.

Report No. 4A-CI-00-09-052

Date: August 10, 2009

This final audit report discusses the results of our review of the information technology security controls of the U.S. Office of Personnel Management's (OPM) Integrated Security Management System (ISMS). Our conclusions are detailed in the "Results" section of this report.

The results of our audit are summarized below:

- OPM's legacy physical security system, Identipass, was decommissioned on January 23, 2009, and was replaced by the new ISMS system on that date. ISMS went through a certification and accreditation process prior to being placed into production. Although an accreditation statement was signed prior to placing the system into production, a certification letter had not been signed at this time. The certification letter for ISMS was signed retroactively by OPM's acting Information Technology Security Officer.
- A security categorization analysis was performed for ISMS. We determined that this evaluation was compliant with Federal Information Processing Standards Publication 199 and National Institute of Standards and Technology (NIST) requirements, and agrees with the overall security categorization of moderate for ISMS.
- An information system security plan was developed for ISMS using the security plan template outlined in the NIST Special Publication 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems.

- An independent security control test and evaluation was performed for ISMS during the certification and accreditation process.
- A self-assessment of security controls was not required for ISMS in fiscal year 2009.
- A contingency plan has been developed and tested for ISMS. However, the contingency plan could be improved with additional details for the recovery procedures and by assigning specific individuals to the recovery teams outlined in the contingency plan.
- A plan of action and milestones document has been created for ISMS to track security weaknesses of the system, although it did not prioritize the identified security weaknesses.
- We independently tested 22 security controls for ISMS and found that 4 of the security controls were not in place during the fieldwork phase of the audit. Three of the four failed controls were corrected during the reporting phase of the audit, but the fourth control has not been implemented.

Contents

Introduction

On December 17, 2002, President Bush signed into law the E-Government Act (P.L. 107-347), which includes Title III, the Federal Information Security Management Act (FISMA). It requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the Office of Management and Budget (OMB) the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In accordance with FISMA, we evaluated the information technology (IT) security controls related to the Office of Personnel Management's (OPM) Integrated Security Management System (ISMS).

Background

ISMS is one of OPM's 41 critical IT systems. As such, FISMA requires that the Office of the Inspector General (OIG) perform an audit of IT security controls of this system, as well as all of the agency's systems on a rotating basis.

The Center for Security and Emergency Actions (CSEA) has been designated with ownership of ISMS. ISMS is used to monitor and control employee, visitor, and guest access to OPM's Theodore Roosevelt Building (TRB) in Washington, D.C. The system is also used to limit access into designated restricted or controlled areas within the TRB. The primary component of ISMS is the C*Cure ID Badging system, which utilizes electronic access cards to operate network based access panels, door locks, turnstyles, and card readers.

This was our first audit of the security controls surrounding ISMS. We discussed the results of our audit with CSEA representatives at an exit conference.

Objectives

Our overall objective was to perform an evaluation of security controls for ISMS to ensure that CSEA officials have implemented IT security policies and procedures in accordance with standards established by OPM's Center for Information Services (CIS).

These policies and procedures are designed to assist program office officials in developing and documenting IT security practices that are in substantial compliance with FISMA, as well as OMB regulations and the National Institute of Standards and Technology (NIST) guidance.

OPM's IT security policies and procedures require managers of all major and sensitive systems to complete a series of steps to (1) certify that their system's information is adequately protected and (2) authorize the system for operations. The overall audit objective was accomplished by reviewing the degree to which a variety of these security program steps have been implemented for ISMS, including:

- Certification and Accreditation (C&A);
- Federal Information Processing Standards (FIPS) Publication 199 Analysis;

- Information System Security Plan;
- Independent Security Control Testing and Risk Assessment;
- Security Control Self-Assessment;
- Contingency Planning;
- Plan of Action and Milestones (POA&M) Process; and
- Evaluation of NIST Special Publication (SP) 800-53 Security Controls.

Scope and Methodology

This performance audit was conducted in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures that we considered necessary. The audit covered FISMA compliance efforts of CSEA officials responsible for ISMS, including IT security controls in place as of June 2009.

We considered the ISMS internal control structure in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives.

To accomplish our objective, we interviewed representatives of OPM's CSEA office and other program officials with ISMS security responsibilities. We reviewed relevant OPM IT policies and procedures, federal laws, OMB policies and guidance, and NIST guidance. As appropriate, we conducted compliance tests to determine the extent to which established controls and procedures are functioning as required.

Details of the security controls protecting the confidentiality, integrity, and availability of ISMS are located in the "Results" section of this report. Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the ISMS system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM IT Security Policy;
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- NIST SP 800-12, An Introduction to Computer Security;
- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems;
- NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems;

- NIST SP 800-60 Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories;
- Federal Information Processing Standard 199, Standards for Security Categorization of Federal Information and Information Systems; and
- Other criteria as appropriate.

In conducting the audit, we relied to varying degrees on computer-generated data. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. However, nothing came to our attention during our audit testing utilizing the computer-generated data to cause us to doubt its reliability. We believe that the data was sufficient to achieve the audit objectives. Except as noted above, the audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States.

The audit was performed by the OPM Office of the Inspector General, as established by the Inspector General Act of 1978, as amended. The audit was conducted from April through July 2009, in OPM's Washington, D.C. office.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether CSEA's management of ISMS is consistent with applicable standards. Nothing came to the OIG's attention during this review to indicate that CSEA is in violation of relevant laws and regulations.

Results

This section details the results of our audit of ISMS.

I. Certification and Accreditation

OPM's legacy physical security system, Identipass, was decommissioned on January 23, 2009, and was replaced by the new ISMS system on that date.

The security certification process for ISMS was facilitated by contractors from the Department of Treasury's Bureau of Public Debt (BPD). On January 22, 2009, a representative from BPD signed a memorandum stating that the security certification work was complete, and that the package was ready for official certification and accreditation via the signing of a certification letter and accreditation memo. On January 23, the ISMS Designated Accrediting Authority (DAA) signed an accreditation statement authorizing the system to operate. However, a certification letter had not been signed at this time. The certification letter for ISMS was signed retroactively by OPM's acting Information Technology Security Officer (ITSO) on March 30, 2009.

NIST SP 800-37 suggests that the certification agent, which at OPM has traditionally been the ITSO, review the complete certification package prior to accreditation phase. The authorizing official relies on the ITSO's input from the security accreditation phase to determine the risk to agency operations, agency assets, or individuals.

For future C&As of ISMS, the ITSO should review the certification package and sign the certification statement prior to presenting the package to the DAA for authorization.

II. Federal Information Processing Standards Publication 199 Analysis

FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, requires the formal categorization of information systems to ensure that the appropriate levels of information security controls are implemented.

NIST SP 800-60 Volume I "Guide for Mapping Types of Information Systems to Security Categories," provides an overview of the security objectives and impact levels identified in FIPS Publication 199.

The security categorization analysis for ISMS considered the potential level of impact (*low, moderate, high*) that would result from a loss of confidentiality, integrity, or availability of the system.

The OIG determined that this evaluation was compliant with FIPS Publication 199 and NIST requirements, and agrees with the overall security categorization of moderate for ISMS.

III. Information System Security Plan

FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, specifies the security requirements that must be implemented on all federal information systems. Federal agencies must implement the minimum security requirements defined in FIPS Publication 200 through the use of the security controls outlined in NIST SP 800-53, Recommended Security Controls for Federal Information Systems. NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in an information systems security plan (ISSP) for each system, and provides guidance for doing so.

BPD developed the ISSP for ISMS utilizing the security plan template outlined in NIST SP 800-18. The ISMS ISSP was reviewed and approved by the system's Designated Security Officer (DSO) and DAA on January 23, 2009. In accordance with NIST SP 800-18, the ISMS ISSP contained the following elements:

- System Name and Identifier;
- System Categorization;
- System Owner;
- Authorizing Official;
- Assignment of Security Responsibility;
- System Operational Status;
- Information System Type;
- General Description/Purpose;
- System Environment;
- System Interconnection/Information Sharing; and
- Laws, Regulations, and Policies Affecting the System.

The ISSP also outlines the information security controls that are implemented or planned to be implemented for ISMS. For each of the 17 security control families outlined in NIST SP 800-53, the ISMS security plan describes the manner in which these control objectives are satisfied for this system.

IV. Independent Security Control Testing and Risk Assessment

As part of the C&A process, BPD conducted a risk assessment and security control testing and evaluation for ISMS. We believe that the testing and evaluation by BPD addressed the critical elements suggested for the risk assessment process by NIST SP 800-30, Risk Management Guide for Information Technology Systems.

BPD developed a Security Assessment Plan (SAP) to document the methodology and scope for the security control testing. The SAP outlines the various assessment methods to be used during the review, and details the procedures to be followed during the risk assessment activities. The testing procedures included, but were not limited to, examining and reviewing assessment objects, interviewing individuals with ISMS security and operational responsibility, and exercising assessment objects under specified conditions to

compare actual with expected behavior. BPD also conducted an automated vulnerability scan of the servers housing ISMS using Retina network vulnerability scanner.

The security control testing was conducted by BPD employees who are independent from ISMS and the CSEA program office that owns the system. BPD created a baseline of security controls that are applicable to ISMS based on its FIPS Publication 199 security categorization of 'moderate.' The tested security controls were derived from NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems. The OIG verified that the appropriate controls were included in the scope of this review. For each tested control, BPD determined whether the control objective was fully satisfied, partially satisfied, or not applicable.

The results of the security control testing were recorded in a Security Assessment Report (SAR). The SAR contains assessment of the risk associated with the security weaknesses found during the assessment along with recommendations for addressing these weaknesses. The vulnerabilities and weaknesses detected during the testing process were grouped into 14 itemized findings, each weighted with a high, medium, or low risk rating. These findings were appropriately transferred to the ISMS POA&M.

V. Security Control Self-Assessment

FISMA requires that the NIST SP 800-53 security controls of each federal information system be tested on an annual basis. In December 2008, an independent contractor conducted a test of ISMS's management, operational, and technical controls as outlined in NIST SP 800-53. Therefore, an internal self-assessment of these controls was not required in fiscal year (FY) 2009. The OIG will verify that a self-assessment of NIST SP 800-53 controls is conducted for this system in FY 2010 as part of the 2010 general FISMA audit process.

See section IV for a review of the independent security controls test for ISMS.

VI. Contingency Planning

NIST SP 800-34, Contingency Planning Guide for IT Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. The OPM IT security policy requires that OPM general support systems and major applications have viable and logical disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

CSEA has documented a contingency plan for ISMS that contains procedures to recover the system following a disruption. Although the ISMS contingency plan contains the majority of critical elements suggested by the NIST guide, several areas of the contingency plan could be improved with additional details and more specific instructions.

Two steps within the contingency plan's procedures to return to normal operations are to "Install latest application code on application servers" and to "Test application to ensure

business needs are met . . . ." However, there are no further instructions on how these steps should be completed.

Failure to itemize the detailed steps involved in the recovery process increases the risk that the recovery team will encounter problems or delays in restoring the system. NIST SP 800-34 states that "Recovery procedures should be written in a straightforward, step-by-step style. To prevent difficulty or confusion in an emergency, no procedural steps should be assumed or omitted. A checklist format is useful for documenting the sequential recovery procedures and for troubleshooting problems if the system cannot be recovered properly."

In addition, the ISMS contingency plan establishes several teams assigned to participate in recovering ISMS operations, but the contact list (call tree) within the document does not identify which individuals are assigned to the various teams. Failure to properly assign individuals to specific teams increases the risk that recovery team members will not be aware of their specific responsibilities in a disaster recovery situation. NIST SP 800-34 states that "Personnel to be notified should be clearly identified in the contact lists appended to the plan. This list should identify personnel by their team position, name, and contact information (e.g., home, work, and pager numbers, e-mail addresses, and home addresses)."

The ISMS contingency plan was tested on May 28, 2009. The test was a table-top exercise that involved a simulated walkthrough of the steps outlined in the contingency plan. Although CSEA documented the simulated results for each component of the contingency plan, the testing report did not contain the detailed step-by-step approach suggested by NIST guidance.

Recommendation 1

We recommend that CSEA continue to develop and improve the ISMS contingency plan. This includes, but is not limited to, adding specific and detailed steps to the recovery procedures and assigning specific individuals to the various recovery teams. CSEA should conduct another test of the contingency plan after the plan has been modified.

CSEA Response:

"Concur. The ISMS contingency plan will continue to be developed and improved as the system and network evolve and lessons learned result in continued improvements. The current ISMS Contingency Plan has been updated to include specific recovery steps and to assign specific individuals to roles and teams. A follow-up exercise was conducted to test the added procedures. Updated Contingency Plan and most recent Contingency Plan test results are included in the accompanying data disc."

OIG Reply:

We acknowledge the steps CSEA has taken to improve the ISMS contingency plan. However, the updated version of the contingency plan continues to lack specific

instructions for several recovery procedures. For example, one step reads "Test all applications associated with the entire ISMS," but no further instructions are provided.

In addition, the updated contingency plan does not assign specific individuals to the four recovery teams (data management team, storage recovery team, applications recovery team, and business interface team). Job titles were added for each individual on the call tree, but there is no indication of which team these individuals are assigned to.

We continue to recommend that CSEA improve the contingency plan for ISMS. We will follow up on the status of this recommendation as part of the FY 2010 FISMA audit.

VII. Plan of Action and Milestones Process

As part of the C&A Process, BPD provided CSEA with a POA&M document outlining 14 security weaknesses detected during the C&A security control testing. All weaknesses and vulnerabilities detected during the C&A process were appropriately included on the ISMS POA&M. Although this POA&M generally adhered to the POA&M format required by OPM's CIS, the ISMS POA&M did not prioritize the identified security weaknesses.

On March 13, 2009, CSEA updated the ISMS POA&M and submitted it to CIS for the FY 2009 second quarter FISMA report to OMB. The March 13 POA&M indicated that all 14 weaknesses had been addressed.

For each of the security weaknesses labeled as "closed", the OIG verified that adequate "proof of closure" (evidence that the weakness has been alleviated) was provided to OPM's CIS. The OIG also independently verified that the proof of closure documentation adequately supports CSEA's position that each of the controls is now in place.

Recommendation 2

We recommend that ISMS edit its POA&M template to facilitate the prioritization of weaknesses.

CSEA Response:

"Concur. CSEA has edited its current POA&M list, which serves as the CSEA ISMS POAM template, to include a column called 'Priority/Risk' to facilitate a risk-based prioritization of remediation activities. A copy of the current CSEA ISMS POA&M List is included in the accompanying data disc."

OIG Reply:

We acknowledge the steps that CSEA has taken to improve the ISMS POA&M. No further action is required.

VIII. NIST SP 800-53 Evaluation

NIST SP 800-53 provides guidance for implementing a variety of security controls for information systems supporting the federal government. The OIG tested a subset of these controls for ISMS as part of this audit, including:

- AT-3: Security Training
- AU-1: Audit and Accountability
- AU-2: Auditable Events
- CA-2: Security Assessments
- CA-4: Security Certification
- CA-5: Plan of Action and Milestones
- CA-6: Security Accreditation
- CM-3: Configuration Change Control
- CM-4: Monitoring Configuration Changes
- CM-6: Configuration Settings
- CP-2: Contingency Plan
- CP-3: Contingency Plan Testing
- IA-4: Identifier Management
- MP-5: Media Transport
- PE-2: Physical Access Authorizations
- PE-8: Access Records
- PL-2: System Security Plan
- PL-4: Rules of Behavior
- PL-5: Privacy Impact Assessment
- PS-4: Personnel Termination
- RA-5: Vulnerability Scanning
- SC-2: Application Partitioning

These controls were evaluated by interviewing individuals with ISMS security responsibilities, reviewing documentation and system screenshots provided by CSEA, viewing demonstrations of system capabilities, and conducting tests directly on the system.

Although it appears that CSEA has successfully implemented the majority of NIST SP 800-53 security controls for ISMS, several tested controls were not fully satisfied:

a) AU-1 Audit and Accountability Policy and Procedures

CSEA has established audit procedures for ISMS that state the system administrator must review audit logs on a weekly basis to search for suspicious activity. However, during the fieldwork phase of this audit, there was a single system administrator with the ability to retrieve system logs, and no procedures in place to review the activity of this administrator. The administrator was the only individual with the ability to change ISMS's sensitive application-level settings, and was also the only individual capable of reviewing this activity. A second individual has since been assigned administrator privileges.

NIST SP 800-53 Revision 2 requires that each system have a "formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance . . . ."

Recommendation 3

We recommend that CSEA expand the ISMS audit procedures to include a process for reviewing the activities of the system administrator.

CSEA Response:

"Concur. An update was made to the CSEA ISMS Audit Procedures, which define the role of an Alternate System Administrator and the responsibility and process/procedures to review the ISMS audit logs on at least a monthly basis. The updated audit procedures are included in the accompanying data disc."

OIG Reply:

We acknowledge the steps that CSEA has taken to improve the ISMS audit procedures. No further action is required.

b) IA-4 Identifier Management

ISMS user accounts exist that are shared by multiple individuals. Although the accounts were not administrator accounts, they did have access privileges that, if abused, could jeopardize ISMS's ability to ensure physical security of OPM facilities. Although one shared account was disabled during the fieldwork portion of this audit, a second shared account still exists.

NIST SP 800-53 Revision 2 states each system must uniquely identify each user.

Recommendation 4

We recommend that CSEA disable all shared user accounts for ISMS, and enforce the use of individual accounts for all users.

CSEA Response:

"Concur. All shared accounts have been disabled or deleted. A screen shot (ISMS User Report 6-29-09.pdf) is included in the accompanying data disc."

OIG Reply:

We acknowledge the steps that CSEA has taken to disable shared user accounts. No further action is required.

c) CM-3/6 Configuration Change Control/Configuration Settings

CSEA has established account management procedures for ISMS that state "Configuration management responsibilities include maintaining an updated baseline configuration for the ISMS (C*CURE) applications and then tracking changes as they occur." However, no baseline configuration exists. In addition, although ISMS automatically logs changes to configuration settings, no procedures exist to formally approve and manage configuration changes.

NIST SP 800-53 states that organizations should document a system's baseline configuration settings, and manage configuration changes using a process that involves formally evaluating and approving each change.

Recommendation 5

We recommend that CSEA document a baseline configuration for ISMS's application level settings and develop procedures for requesting and approving changes to these settings.

CSEA Response:

"Concur. The baseline configuration for ISMS has been developed and procedures for Configuration Management are contained in section 4.B of the updated 'CSEA ISMS, System and Account Management Procedures' dated July 6, 2009."

OIG Reply:

Although the updated System and Account Management Procedures contain procedures for requesting and approving configuration changes, CSEA's response to the draft report did not contain evidence indicating that a baseline system configuration has been documented.

We continue to recommend that CSEA document a baseline configuration for ISMS's application level settings. We will follow up on the status of this recommendation as part of the FY 2010 FISMA audit.

d) PL-4 Rules of Behavior

CSEA has established a set of rules for ISMS that describes their responsibilities and expected behavior with regard to information system usage. However, not all ISMS users have formally acknowledged their understanding of the rules of behavior.

NIST SP 800-53 states that system owners must receive "signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior . . . ."

Recommendation 6

We recommend that CSEA have all ISMS users sign the rules of behavior document.

CSEA Response:

"Concur. All ISMS users (federal employees and contract guard personnel) have signed the Rules of Behavior document."

OIG Reply:

We acknowledge the steps that CSEA has taken to have ISMS users sign a rules of behavior document. No further action is required.

Major Contributors to this Report

This audit report was prepared by the U.S. Office of Personnel Management, Office of Inspector General, Information Systems Audits Group. The following individuals participated in the audit and the preparation of this report:

- [redacted], Group Chief
- [redacted], Auditor-in-Charge

Appendix

July 15, 2009

MEMORANDUM FOR [redacted]
Auditor-in-Charge
Information Systems Audit Group
Office of Inspector General

FROM: [redacted]
Deputy Associate Director
Center for Security and Emergency Actions

Subject: CSEA Response to OPM Office of Inspector General (OIG) Draft Report No. 4A-CI-00-09-52, June 25, 2009.

The Center for Security and Emergency Actions has reviewed the OIG's draft audit report and concurs with the Inspector General's six recommendations to improve the security posture of the Integrated Security Management System (ISMS). The remainder of this memorandum references the individual recommendations and CSEA's actions to implement them.

Evidence supporting the implementation of OIG recommendations are provided on a data disk with this report (Folder: CSEA ISMS OIG Response, July 2009).

Recommendation 1:
Develop and improve the ISMS contingency plan to include, but not limited to:

a. Adding specific and detailed steps to recovery procedures.
b. Assign specific individuals to the various recovery teams.
c. Conduct a follow-up test of the contingency plan after modifications.

Response: Concur
The ISMS contingency plan will continue to be developed and improved as the system and network evolve and lessons learned result in continued improvements. The current ISMS Contingency Plan has been updated to include specific recovery steps and to assign specific individuals to roles and teams. A follow-up exercise was conducted to test the added procedures. Updated Contingency Plan and most recent Contingency Plan test results are included in the accompanying data disc.

Recommendation 2:
OIG recommends that ISMS edit its POA&M template to facilitate the prioritization of weaknesses.

Response: Concur
CSEA has edited its current POA&M list, which serves as the CSEA ISMS POAM template, to include a column called "Priority/Risk" to facilitate a risk-based prioritization of remediation

activities. A copy of the current CSEA ISMS POA&M List is included in the accompanying data disc.

Recommendation 3:
OIG recommends that CSEA expand the ISMS audit procedures to include a process for reviewing the activities of the system administrator.

Response: Concur
An update was made to the CSEA ISMS Audit Procedures, which define the role of an Alternate System Administrator and the responsibility and process/procedures to review the ISMS audit logs on at least a monthly basis. The updated audit procedures are included in the accompanying data disc.

Recommendations 4:
OIG recommends that CSEA disables all shared accounts for ISMS, and enforce the use of individual accounts for all users.

Response: Concur
All shard accounts have been disabled or deleted. A screen shot (ISMS User Report 6-29-09.pdf) are included in the accompanying data disc.

Recommendation 5:
OIG recommends that CSEA document a baseline configuration for ISMS's application level settings, and develop procedures for requesting and approving changes to these settings.

Response: Concur
The baseline configuration for ISMS has been developed and procedures for Configuration Management are contained in section 4.B of the updated "CSEA ISMS, System and Account Management Procedures." dated July 6, 2009.

Recommendation 6:
OIG recommends that CSEA have all ISMS users sign the rules of behavior documents.

Response: Concur
All ISMS users (federal employees and contract guard personnel) have signed the Rules of Behavior document.