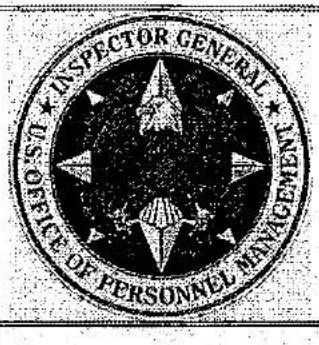

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Subject:

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT FY 2009

Report No. 4A-CI-00-09-031

Date: November 5, 2009

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT
FY 2009

WASHINGTON, D.C.

Report No. 4A-CI-00-09-031

Date: November 5, 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

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT FY 2009

WASHINGTON, D.C.

Report No. 4A-CI-00-09-031

Date: November 5, 2009

This final audit report documents the Office of Personnel Management's (OPM's) continued efforts to manage and secure its information resources. We have significant concerns regarding the overall quality of the information security program at OPM. These concerns are rooted in the lack of adequate information security governance activities in accordance with legislative and regulatory requirements. Specifically, the agency has not fully documented information security policy and procedures or established appropriate roles and responsibilities.

The lack of policies and procedures was reported as a material weakness in the fiscal year (FY) 2007 and FY 2008 Federal Information Security Management Act (FISMA) audit reports. While some progress was made in FY 2009, detailed guidance is still lacking. An updated Information Security and Privacy Policy was finalized in August 2009. This policy outlines the information technology (IT) security controls that should be in place for the major applications owned by the agency. However, the majority of the text in this policy is derived or copied directly from National Institute of Standards and Technology (NIST) guidance and has not been tailored to specifically address OPM's IT environment. In addition, detailed procedures and implementing guidance are still missing.

This year we are expanding the material weakness to include the agency's overall information security governance program and incorporating our concerns about the agency's information security management structure. As of late September 2009, there had been no permanent senior agency information security official (SAISO) in the agency for nearly 18 months. During this time, we observed a serious decline in the quality of the agency's information security program. In addition, there is no permanent Privacy Program Manager assigned to manage the agency's privacy program. As a result, there are many deficiencies in OPM's privacy program.

The agency has recently appointed a new SAISO; however, it remains to be seen whether it will commit the necessary resources and develop the appropriate functions required of this role. We will reevaluate this issue during the FY 2010 FISMA audit.

The continuing weaknesses in OPM's information security program result directly from inadequate governance. Most, if not all, of the exceptions we noted this year resulted from a lack of necessary leadership, policy, and guidance. Our most notable observations include:

- As noted above, OPM continues to lack adequate and up-to-date IT security policies and procedures. We continue to consider this to be a material weakness in OPM's IT security program.
- One system on OPM's inventory was placed into production before a certification and accreditation (C&A) was completed, and the prior C&A for three systems has expired and a new C&A has not been completed. Weaknesses in OPM's C&A process continue to remain a significant deficiency in OPM's IT security program.
- Weaknesses in OPM's privacy impact assessment (PIA) process and the agency's failure to meet privacy-related requirements from the Office of Management and Budget (OMB) lead us to believe that there is a significant deficiency in OPM's management of its privacy program.

In addition to these weaknesses, the OIG noted the following controls in place and opportunities for improvement:

- OPM's Center for Information Services (CIS) maintains a master inventory of OPM's major systems. We generally agree with the number of systems listed in the inventory (42), but we identified at least one major application that does not appear on the system inventory and has not been subject to a C&A. In addition, OPM's system inventory does not identify interfaces between internal and external systems.
- A C&A has been completed and remains active for 38 of the 42 systems in OPM's inventory.
- The IT security controls have been adequately tested for 40 of OPM's 42 systems during FY 2009.
- Four out of OPM's 42 systems did not have an adequately documented and/or up-to-date contingency plan. In FY 2009, the contingency plans for 31 of OPM's 42 systems were tested in full compliance with the requirements of NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems.

- Nothing has come to our attention to indicate that OPM program offices do not maintain oversight of systems operated by a contractor.
- The Plan of Action and Milestones (POA&M) for three OPM systems did not contain all security weaknesses identified during the annual security control tests of those systems.
- POA&Ms are continuously managed for 40 of OPM's 42 systems; current POA&Ms were not submitted to CIS for two systems in the fourth quarter of 2009.
- When closing POA&M items, OPM program offices have provided adequate evidence to CIS that the weaknesses were corrected.
- Five agency systems have POA&M weaknesses with remediation activities over 120 days old.
- Two agency systems did not prioritize weaknesses on their POA&Ms.
- OPM's PIA Guide has not been updated in over three years and fails to address several requirements of OMB Memorandum M-03-22.
- The OIG has not received evidence that system owners review their PIA documentation on an annual basis.
- OPM has implemented a breach notification policy.
- CIS developed a formal plan to reduce the use of social security numbers (SSNs) at OPM. However, the plan does not address participation in government-wide efforts to explore alternatives to agency use of SSNs, as required by U.S. Office of Management and Budget Memorandum M-07-16.
- OPM had developed a standard laptop image that utilizes software-based full-disk encryption. However, CIS was unable to provide evidence of how many laptops issued to OPM employees and contractors contain the new image with encryption capabilities.
- OPM developed a methodology for logging computer-readable data extracts of personally identifiable information.
- Several policies related to configuration management have not been updated in over four years.
- OPM has implemented several techniques for monitoring compliance with configuration management policies.
- OPM has developed a Windows XP image that is generally compliant with Federal Desktop Core Configuration standards. However, this image has not been implemented on any production workstations.
- Language from 48 CFR Part 39, Acquisition of Information Technology, has not been included in all contracts related to common security settings.
- One [redacted] continues to run on an unsupported version of [redacted] without a formally documented risk acceptance.
- OPM has developed an "Incident Response and Reporting Policy" that documents procedures for reporting all IT security events to the appropriate entities.

- CIS has implemented a process to provide annual IT security and privacy awareness training to all OPM employees and contractors.
- OPM's system inventory does not identify all systems that are subject to e-Authentication requirements.

Contents

Introduction

On December 17, 2002, the President signed into law the E-Government Act (Public Law 107-347), which includes Title III, the Federal Information Security Management Act (FISMA). FISMA 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 conducted an evaluation of OPM's security program and practices. As part of our evaluation, we reviewed OPM's FISMA compliance strategy and documented the status of its compliance efforts.

Background

FISMA requirements pertain to all information systems (national security and unclassified systems) supporting the operations and assets of an agency, including those systems currently in place or planned. The requirements also pertain to information technology (IT) resources owned and/or operated by a contractor supporting agency systems.

FISMA reemphasizes the Chief Information Officer's (CIO) strategic, agency-wide security responsibility. At OPM, security responsibility is assigned to the agency's Center for Information Services (CIS), which is managed by the CIO. FISMA also clearly places responsibility on each agency program office to develop, implement, and maintain a security program that assesses risk and provides adequate security for the operations and assets of programs and systems under their control.

To assist agencies and IGs in fulfilling their FISMA evaluation and reporting responsibilities, OMB issued memorandum M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. This memorandum provides a consistent form and format for agencies to report to OMB. It identifies a series of reporting topics that relate to specific agency responsibilities outlined in FISMA. Our evaluation and reporting strategies were designed in accordance with the above OMB guidance.

Objectives

Our overall objective was to perform an evaluation of OPM's security program and practices, as required by FISMA. Specifically, we reviewed the following areas of OPM's IT security program in accordance with OMB's FISMA IG reporting requirements:

- Information Security Governance;
- System Inventory;
- Certification and Accreditation, Security Controls Testing, and Contingency Planning;
- Agency Oversight of Contractor Systems;
- Agency Plan of Action and Milestones Process;
- Certification and Accreditation Process;
- Agency Privacy Program;
- Configuration Management;

- Incident Reporting;
- Security Awareness Training;
- E-authentication Risk Assessments; and
- IT Security Policies and Procedures.

In addition, we evaluated the security controls of three major applications/systems at OPM (see Scope and Methodology for details of these audits). We also followed-up on outstanding recommendations from prior FISMA audits (see Appendix I).

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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit covered OPM's FISMA compliance efforts throughout FY 2009.

We considered the internal control structure for various OPM systems 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.

In conducting our audit, we relied to varying degrees on computer-generated data provided by OPM. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. However, we believe that the data was sufficient to achieve the audit objectives, and nothing came to our attention during our audit testing to cause us to doubt its reliability.

As appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as intended. The results from tests performed on a sample basis were not projected to the universe of controls.

We reviewed OPM's general FISMA compliance efforts in the specific areas defined in OMB's guidance and the corresponding reporting instructions. We also evaluated the security controls for the following three major applications:

- Enterprise Human Resources Integration Data Warehouse (OIG Report No. 4A-HR-00-09-032)
- Electronic Official Personnel File (OIG Report No. 4A-HR-00-09-032)
- Integrated Security Management System (OIG Report No. 4A-CI-00-09-052)

In addition, in May 2009, the OIG issued a Flash Audit Alert (FAA) to OPM's Director highlighting our concerns with the agency's IT security program (report 4A-CI-00-09-053). As part of this audit, we followed up on OPM's progress in implementing recommendations from the FAA.

Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the set of internal controls at OPM taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Security and Privacy Policy Volume 2;
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- OMB Memorandum M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management;
- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information;
- OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- National Institute for Standards and Technology (NIST) Special Publication (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 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 I Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories;
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems;
- FIPS Publication 140-2, Security Requirements for Cryptographic Modules; and
- Other criteria as appropriate.

The audit was performed by the OIG at OPM, as established by the Inspector General Act of 1978, as amended. Our audit was conducted from May through September 2009 in OPM's Washington, D.C. office.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether OPM's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, OPM's CIS and other program offices were not in complete compliance with all standards, as described in the "Results" section of this report.

Results

The sections below detail the results of the OIG's audit of OPM's FISMA compliance efforts. The results are formatted to be consistent with the questions outlined in the FY 2009 OMB Reporting Template for IGs. Throughout this report, we do not reference OPM systems by name, but we have already provided detailed documentation to CIS discussing our concerns and the specific systems involved.

I. Information Security Governance

In May 2009, the OIG issued a Flash Audit Alert (FAA) to OPM's Director highlighting our concerns with the agency's IT security program. An FAA is used when issues have been identified that require the immediate attention of the Director. The four primary issues outlined in the FAA were:

- CIS misrepresented the status of the agency's IT security program in the FY 2009 second quarter FISMA report issued to OMB;
- the agency's security policies and procedures continue to remain severely outdated;
- the IT security program at OPM is understaffed; and,
- the agency has operated without a senior agency information security official (SAISO) for over 14 months (as of May 2009).

In the interim, there has been limited progress in correcting these issues. The underlying cause, in our opinion, is that OPM has not established adequate information security governance activities in accordance with legislative and regulatory requirements. Specifically, the agency has not fully documented information security policy and procedures or established appropriate roles and responsibilities.

The lack of policies and procedures was reported as a material weakness in the FY 2007 and FY 2008 FISMA audit reports. This year we are expanding the material weakness to include the agency's overall information security governance program and incorporating our concerns about the agency's information security management structure.

As of late September 2009, there had been no permanent SAISO in the agency for nearly 18 months. During this time, we observed a serious decline in the quality of the agency's information security program. In addition, there is no permanent Privacy Program Manager assigned to manage the agency's privacy program. As a result, there are many deficiencies in OPM's privacy program. See section **VII** of this report for details.

The agency has recently appointed a new SAISO; however, it remains to be seen whether the agency will commit the necessary resources and develop the appropriate functions required of this role. We will reevaluate this issue during the FY 2010 FISMA audit.

The following section discusses the original FAA recommendations, followed by the management response and current status:

a) **Flash Audit Alert Recommendation 1**

We recommend that CIS correct the FY 2009 second quarter FISMA report to accurately reflect the status of OPM's IT security position as of March 1, 2009.

CIS Response to FAA:

"The Center for Information Services (CIS) security team acted on the best information they had at the time . . . . We agree with the recommendation that OPM report the number of systems with weaknesses more than 120 days overdue, instead of the number of weaknesses. This was a mistake in our understanding of the reporting requirement."

Current Status

We verified that CIS corrected and submitted the FY 2009 second quarter FISMA report. We also verified that the FY 2009 third quarter FISMA report accurately represented the status of OPM's security program at that time.

CIS Response:

"The Center for Information Services (CIS) security team will continue to ensure the quarterly FISMA reports reflect correct and accurate information for OPM's security program."

b) **Flash Audit Alert Recommendation 2**

We recommend that CIS develop a comprehensive set of IT security policies and procedures, and a plan for updating it at least annually.

CIS Response to FAA:

"We agree with this recommendation and have been working for many months to complete needed updates. Work began as soon as funding was provided. Many policies and procedures have already been revised, with the remainder targeted for completion by 8/31/09."

Current Status

OPM's IT security policies and procedures continue to lack adequate current guidance on managing IT security at the agency. See section **XII** of this report for details.

CIS Response:

"Please refer to section XII for our response to Recommendation 30 regarding the IT security policies and procedures."

c) **Flash Audit Alert Recommendation 3**

We recommend that the OPM Director ensure that CIS has adequate resources to properly staff its IT Security and Privacy Group.

CIS Response to FAA:

"We agree with this recommendation. As we discussed with OIG staff on numerous occasions, CIS has been working with HR for more than a year to reorganize and elevate the IT security function, to upgrade the level of the IT security officer from a GS-14 to a GS-15, and to add staff. A new organizational alignment, grade structure and resources for the IT Security and Privacy Group were approved on March 4, 2009. Under this new structure, the IT security staff will grow from 3 to 6. We consider this recommendation to be closed."

Current Status

The organizational realignment of OPM's IT security function remains incomplete, and we continue to believe that CIS lacks the resources needed to manage an adequate IT security program. Eleven of the 19 audit recommendations issued in the FY 2008 FISMA audit report have been rolled forward into this FY 2009 FISMA report, indicating that CIS does not have the resources needed to remediate identified security weaknesses.

CIS Response:

"We agree with this recommendation. Currently the IT security group lacks the resources necessary to establish and maintain an effective security and privacy program. The new SAISO . . . that was hired in September 2009 has identified resources needed and his recommendations are under review with senior management. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-27)."

d) Flash Audit Alert Recommendation 4

We recommend that CIS recruit a permanent Senior Agency Information Security Officer as soon as possible, and adequate staff to effectively manage the agency's IT security program.

CIS Response to FAA:

"We agree with this recommendation. Recruiting has been in progress since the reorganization was approved. We have made a couple of offers to fill the GS-15 and GS-14 positions, which were declined. We have identified another excellent candidate for the GS-15 position. We are currently in the process of getting Chief of Staff approval to extend an offer. We are targeting a report date in August."

Current Status

CIS hired a permanent SAISO in September 2009. However, the agency operated with an acting SAISO for over 11 months of FY 2009. In addition, the organization of the staff reporting to the SAISO has not been finalized. On a potentially positive note, the OPM Director has recently appointed a new Acting Chief Information Officer, who has

developed preliminary plans to expand and improve OPM's IT security program. We will reevaluate these developments during the FY 2010 FISMA audit.

CIS Response:

"We agree with this recommendation. Currently the IT security group lacks the resources and the organizational structure necessary to establish and maintain an effective security and privacy program. The new SAISO . . . that was hired in September 2009 has developed an organizational chart, roles and responsibilities and resources needed. His recommendations are under review with senior management. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. As referenced in Flash Audit Alert Recommendation 3, we have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-27) regarding resources."

II. System Inventory

OPM has identified 42 major applications/systems within 8 of its program offices. OPM's system inventory indicated that these 42 systems were comprised of the following FIPS Publication 199 system impact classifications: 7 high, 33 moderate, and 2 low. The inventory also indicated that 32 systems operated within the agency and 10 are operated at a contractor facility.

CIS continuously maintains a master inventory of OPM's major systems, and sends monthly reminders to the various program offices asking for updates on the status of systems included in the inventory. CIS also facilitates the process of adding new systems to the inventory and removing decommissioned systems.

The quality of OPM's system inventory has greatly improved since it was reviewed during the OIG FY 2008 FISMA audit. Several fields have been added to the inventory spreadsheet to clearly identify the status of each system (production, development, planning) along with the name and contact information of individuals with security and ownership responsibility. In addition, a revision history has been added to the inventory to track specific updates and facilitate version control of the master inventory document.

The OIG generally agrees with the total number of systems listed in the most recent system inventory (42) and agrees with the number of systems identified as operated by a contractor (10). However, we identified at least one major application that does not appear on the system inventory and has not been certified and accredited (C&A).

OPM's system inventory does not identify interfaces between internal and external systems, and the agency does not have a policy related to security agreements between interfacing systems. OPM's Information Security and Privacy Policy Volume 2 states that "this policy applies to other agency's systems as delineated in memorandums of understanding (MOUs) and interconnection security agreements (ISAs) with OPM." However, this policy does not provide any guidance outlining the appropriate use of MOUs and ISAs (required elements of these agreements, when they are required, etc).

In addition, CIS identified 21 systems used by OPM but owned and maintained by another federal agency. However, this list was compiled at the request of the OIG in September 2009 and is not complete.

Recommendation 1

We recommend that CIS conduct a survey of OPM program offices (particularly the Benefits Systems Group) to identify any systems that exist but do not appear on the system inventory. The systems discovered during this survey should be promptly added to the system inventory and certified and accredited.

CIS Response:

"We agree with this recommendation. The IT Security and Privacy group will conduct a network assessment to map out the OPM network and identify all missing systems and created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-28)."

Recommendation 2

We recommend that CIS develop and maintain an inventory of all system interfaces.

CIS Response:

"We agree with this recommendation. The IT Security and Privacy team will include system interface information on the OPM FISMA Master System Inventory going forward. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-29). Please note as stated in response to IG Information Request #24, system interface information is included within each System Security Plan for each system currently on the OPM FISMA Master System Inventory."

Recommendation 3

We recommend that CIS develop a policy providing guidance on the development and appropriate use of MOUs and ISAs.

CIS Response:

"We agree with this recommendation. Currently the IT Security and Privacy group lacks the resources necessary to establish and maintain an effective security and privacy program. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-30)."

Recommendation 4

We recommend that CIS conduct a survey to determine how many systems owned by another agency are used by OPM.

CIS Response:

"We agree with this recommendation. We have made some progress with this task (please refer to IG Information request #24) but we lack the resources to conduct a complete network assessment to map out the OPM network and identify all systems. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-31)."

III. Certification and Accreditation, Security Controls Testing, and Contingency Planning

a) Number of systems certified and accredited

A C&A has been completed and remains active for 38 of the 42 systems in OPM's inventory. See section **VI** below for details of the systems without a current C&A and a review of OPM's C&A process.

b) Number of systems for which security controls have been tested in the past year

NIST SP 800-53 Revision 2 outlines the security controls that should be implemented for federal information systems. FISMA requires each agency to perform for all systems "Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually . . . ."

An annual test of security controls provides a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. Failure to complete a security controls test increases the risk that agency officials are unable to make informed judgments to appropriately mitigate risks to an acceptable level.

We conducted a review of the documentation resulting from the test of security controls for each system in OPM's inventory. In addition, we judgmentally selected specific controls tested in FY 2009 from various systems and independently evaluated whether the controls have been implemented. Our evaluation indicated that the IT security controls had been adequately tested for 40 of OPM's 42 systems during FY 2009.

The quality of the security control tests among OPM's systems varied significantly, and many different formats and templates were used to document the tests. We believe that this variance is a result of OPM's lack of agency-wide policy or guidance on how to adequately test its systems' security controls.

Recommendation 5

We recommend that CIS develop a policy for adequately testing the security controls of OPM's systems, and provide training to the Designated Security Officer (DSO) community related to proper security control testing.

CIS Response:

"We agree with this recommendation. Currently the IT security group lacks the resources necessary to establish and maintain these policies and training program. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-32)."

Recommendation 6 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 1)*

We recommend that OPM ensure that an annual test of security controls has been completed for all systems. The IT security controls should be immediately tested for the two systems that were not subject to testing in FY 2009.

CIS Response:

"We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-1."

c) Number of systems which have a contingency plan tested in accordance with policy

FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. In addition, the OPM Certification and Accreditation Guide states that "To fully address system security throughout the certification and accreditation process, various security documents are required to be created and maintained throughout the life of the system." The Guide states that one of the required security documents is a contingency plan.

Four out of OPM's 42 systems did not have an adequately documented and/or up-to-date contingency plan. One system was missing a contingency plan, one system did not have an updated contingency plan after going through a major infrastructure change, and two systems were placed into production before a contingency plan was developed.

In FY 2009, the contingency plans for 31 of OPM's 42 systems were tested in full compliance with the requirements of NIST SP 800-34, Contingency Planning Guide for Information Technology Systems. Of the remaining 11 systems, 4 were not subject to any form of contingency plan test in FY 2009, and 7 were tested, but not with a scenario-based contingency plan test conducted in accordance with NIST SP 800-34 requirements.

OPM's Information Security and Privacy Policy Volume 2 states that each system owner must "Test the contingency plan for the information system at least annually to determine the plan's effectiveness and the system's readiness to execute the plan." However, this

policy does not provide instructions for conducting the contingency plan test in accordance with NIST guidance or a standard template for reporting the results.

Effective contingency planning and testing establishes procedures and technical measures that enable a system to be recovered quickly and effectively from a service disruption or disaster. An incomplete or untested contingency plan increases the risk that a system could not recover from a service disruption in a timely manner.

Recommendation 7

We recommend that OPM develop detailed guidance related to developing and testing the contingency plans of agency systems and provide training to the DSO community related to proper contingency planning and contingency plan testing.

CIS Response:

"We agree with this recommendation. Currently the IT security group lacks the resources necessary to establish and maintain these policies and training program. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-33)."

Recommendation 8

We recommend that up-to-date contingency plans be developed for all agency systems.

CIS Response:

"We agree with this recommendation. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-34)."

Recommendation 9 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 2)*

We recommend that OPM's program offices test the contingency plans for each system on an annual basis. The contingency plans should be immediately tested for the 11 systems that were not subject to testing in FY 2009.

CIS Response:

"We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-2."

IV. Agency Oversight of Contractor Systems

Ten of OPM's 42 systems are operated by a contractor, and each of these systems has been certified and accredited by OPM. Nothing has come to our attention to indicate that OPM program offices do not maintain oversight of systems operated by a contractor. However, the agency does not have a formal policy providing guidance on the appropriate oversight of contractors and contractor-run systems.

Recommendation 10

We recommend that OPM develop a policy providing guidance on providing adequate oversight of contractor operated systems.

CIS Response:

"We agree with this recommendation. Currently the IT security group lacks the resources necessary to establish and maintain these policies and provide the oversight needed. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-35)."

V. Agency Plan of Action and Milestones Process

A plan of action and milestones (POA&M) is a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for IT security weaknesses. The sections below detail several weaknesses related to the appropriate use of POA&Ms at OPM. These weaknesses consist of items that are the responsibility of both CIS and the various program offices owning the information systems.

a) Policy for establishing a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts

Although CIS has provided informal guidance to OPM program offices related to the POA&M process, they have not published a formal policy that documents how POA&Ms should be managed at the agency. OPM has developed a draft version of "Plan of Action and Milestone Standard Operating Procedures," but this policy has not been published to OPM's internal website (THEO), and the agency's DSO community has not received training related to the new POA&M procedures.

Recommendation 11

We recommend that CIS publish the Plan of Action and Milestone Standard Operating Procedure to THEO. Once the procedures have been published, CIS should work closely with the DSO community, providing training and information-sharing sessions, to implement the procedures and ensure that there is a clear understanding of the appropriate management of POA&Ms.

CIS Response:

"We agree with this recommendation. We have created a CIS POA&M item to document the completion of this recommendation (CIS POAM FY09-Q4-CIS-36). The POA&M Guide has been published as of September 2009 on Theo - http://theo.opm.gov/policies/ispp/FINAL_POAM_Process_SOP_093009.pdf"

OIG Reply:

We acknowledge the steps that CIS has taken to publish the POA&M Guide to THEO and continue to recommend that CIS work closely with the DSO community, providing training and information-sharing sessions, to implement the procedures and ensure that there is a clear understanding of the appropriate management of POA&Ms.

b) POA&M as an agency-wide process incorporating all known IT security weaknesses

In FY 2008, the OIG conducted audits of 4 OPM systems with a total of 13 audit recommendations. We found that all 13 recommendations were included in the appropriate system's POA&Ms. In addition, we verified that all of the recommendations made during the FY 2008 FISMA audit were incorporated into the CIS POA&M. However, we found that the POA&Ms for three OPM systems did not contain all security weaknesses identified during the annual security control tests of those systems.

Recommendation 12 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 4)*

We recommend that OPM program offices incorporate all known IT security weaknesses into POA&Ms.

CIS Response:

"We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-4. Since the POA&M SOP was just recently published on Theo, we will continue to assist program offices through this process."

c) Management of POA&Ms by program offices

OPM program offices are responsible for developing, implementing, and managing POA&Ms for each system that they own and operate. We were provided evidence that POA&Ms are continuously managed for 40 of OPM's 42 systems; current POA&Ms were not submitted to CIS for 2 systems in the fourth quarter of 2009.

Recommendation 13 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendations 5 and 6)*

We recommend that an up-to-date POA&M exist for each system in OPM's inventory, and that system owners submit updated POA&Ms to CIS on a quarterly basis.

CIS Response:

"We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-5 and CIS POAM FY09-Q1-CIS-6. The POA&M SOP has been published as of September 2009 which provides guidance to DSO's regarding POA&M submission. Please note that since OMB did not require any POA&M submissions for FY09 quarter 4, CIS did not continue to follow up with program offices to ensure submissions were provided to CIS for FY09 quarter 4."

d) Remediation of system deficiencies in a timely manner

Each program office is required to place all security deficiencies on POA&Ms and for each deficiency must indicate when they expect the deficiency to be remediated. Although the majority of program offices remediated POA&M deficiencies in a timely manner, there are significantly overdue remediation efforts for several systems; see section (f), below.

e) Effectiveness of deficiency remediation plans in correcting the security weakness

When a POA&M item is remediated, the program offices are required to submit a work completion plan and evidence that the deficiency is corrected to CIS for review. We reviewed work completion plans for 10 systems and found that all 10 provided sufficient evidence that the weakness was corrected.

f) Compliance with estimated dates for remediation

We reviewed the POA&Ms for all OPM systems and determined that 5 agency systems have POA&M weaknesses with remediation activities over 120 days overdue. This indicates that CIS has not provided adequate leadership to ensure that program offices assign reasonable due dates and stay on track to meet those dates. Program offices are equally responsible for dedicating adequate resources to addressing POA&M weaknesses and meeting target objectives.

Recommendation 14

We recommend that CIS develop a formal corrective action plan to immediately remediate all POA&M weaknesses that are over 120 days overdue. In addition, we recommend that CIS take a lead role in the future and work closely with OPM program offices to ensure that POA&M completion dates are achieved.

CIS Response:

"We agree with this recommendation. The POA&M SOP has been published as of September 2009 which provides guidance to DSO's regarding POA&M management. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-37) on supplemental guidance to the DSO's."

g) Agency CIO centrally tracks, maintains, and reviews POA&M activities on a quarterly basis

CIS requires program offices to provide the evidence, or "proof of closure," that security weaknesses have been resolved before closing the related POA&M.

We selected POA&M items from 10 systems and reviewed the proof of closure documentation provided by the program offices when the POA&M items were closed. The 10 systems were selected from a universe of 42 systems and were judgmentally

chosen by OIG auditors. Although the results of the sample test were not projected to the entire population, nothing came to our attention to indicate that program offices are not providing adequate proof of closure to CIS when closing POA&M items.

h) POA&M process prioritizes IT security weaknesses

Each program office at OPM is required to prioritize IT security weaknesses on their POA&Ms to help ensure significant IT security weaknesses are addressed in a timely manner. However, we found that two agency systems did not prioritize weaknesses on their POA&Ms.

Recommendation 15

We recommend that the program offices responsible for the two systems in question prioritize the system weaknesses listed on their POA&Ms.

CIS Response:

"We agree with this recommendation. The POA&M SOP has been published as of September 2009 which provides guidance to DSO's regarding prioritizing weaknesses. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-38) on supplemental guidance to the DSO's."

VI. Certification and Accreditation Process

Certification is a comprehensive assessment that attests that a system's security controls are meeting the security requirements of that system, and *accreditation* is the official management decision to authorize operation of an information system and accept its risks. Each major application at OPM is subject to the certification and accreditation (C&A) process every three years.

We reviewed the C&A documentation for all OPM systems subject to a C&A in FY 2009. During this review we found that OPM program offices generally adhered to the requirements of OPM's C&A guide, and presented the authorizing official with complete and reliable C&A information to facilitate an informed system authorization to operate. However, we discovered that one system on OPM's inventory was placed into production before a C&A was completed, and the prior C&A for three systems has expired and a new C&A has not been completed.

In addition, the OIG disagrees with the security categorization of one system whose C&A was conducted in FY 2009. The system was categorized as "Low," but should have been classified as "Moderate" because the system contains personal identity information that could result in serious harm to individuals if it were disclosed.

According to OPM's C&A policy, "all OPM divisions and offices must formally certify and accredit all major and minor applications and general support systems." It is the responsibility of OPM's CIS to ensure that all live/production systems at OPM are subject to

a complete C&A every three years, as required by FISMA. The FY 2008 OIG FISMA audit report stated that weaknesses in OPM's C&A process are a significant deficiency in the control structure of the agency's IT security program. We believe that this issue continues to be a significant deficiency in FY 2009.

Recommendation 16 ***(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 9)***

We recommend that all active systems in OPM's inventory have a complete and current C&A.

CIS Response:

"We agree with this recommendation. The IT Security and Privacy group would like to conduct a network assessment to map out the OPM network and identify all systems and account for missing C and A's but we currently lack the resources to perform this task. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We are tracking this effort under CIS POAM FY09-Q1-CIS-9."

Recommendation 17

We recommend that the FIPS Publication 199 security categorization be updated for the inappropriately categorized system.

CIS Response:

"We agree with this recommendation. The Center for Information Services (CIS) security team will work with the DSO's to ensure the FIPS 199 reflect the appropriate rating. During the monthly October 2009 Information Technology Security Working Group (ITSWG) meeting, the writer and subject matter expert from NIST provided a briefing on NIST 800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories) to the DSO's and CIS. We have created a CIS POA&M item to continue to track our progress (CIS POAM FY09-Q4-CIS-39)."

VII. Agency Privacy Program

The OIG evaluated OPM's privacy program by conducting a qualitative assessment of the agency's privacy impact assessment (PIA) process and its progress in implementing the requirements of privacy-related OMB Memoranda.

a) Privacy Impact Assessments

The E-Government Act of 2002, section 208, requires agencies to conduct privacy impact assessments (PIA) of information systems that process personally identifiable information (PII). OMB Memorandum M-03-22 provides guidance on implementing the privacy provisions of the E-Government Act of 2002, including PIAs.

OPM has developed a PIA Guide that outlines the process for conducting a PIA for agency systems. However, the PIA Guide has not been updated in over three years, and fails to address several requirements of OMB Memorandum M-03-22, including:

- PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA; and
- PIAs for major applications should reflect more extensive analyses of:
  - the consequences of collection and flow of information;
  - the alternatives to collection and handling as designed;
  - the appropriate measures to mitigate risks identified for each alternative; and
  - the rationale for the final design choice or business process.

Although PIAs are only required for systems that collect or maintain information in identifiable form about members of the general public, OMB encourages agencies to conduct PIAs of systems that process sensitive information about government employees and contractors. However, OPM's PIA Guide does not provide guidance for evaluating which, if any, of these additional systems should be subject to a PIA.

The PIA Guide also states that each system owner must review their existing PIA documentation on an annual basis, and submit evidence of the review to CIS by September 1 of each year. However, the OIG has not received evidence that this review has been completed for any OPM systems. In addition, one new system was placed into production in FY 2009 without a PIA signed by the CIO.

Recommendation 18

We recommend that CIS update the PIA Guide to address all of the requirements of OMB Memorandum M-03-22.

CIS Response:

"We agree with this recommendation. The privacy group is currently working on a new PIA Guide and a new PIA Template. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-40)."

Recommendation 19

We recommend that CIS conduct a new PIA survey to determine which OPM systems require a PIA, including those systems that process sensitive information about government employees and contractors.

CIS Response:

"We agree with this recommendation. The IT Security and Privacy group would like to conduct a network assessment to identify all PII information present on the OPM network but we currently lack the resources to perform this task. The network assessment would be followed by a request to each office that owns the PII to conduct privacy threshold analysis (PTA). The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We

have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-41)."

Recommendation 20

We recommend that a new PIA be conducted for the appropriate systems based on the updated PIA Guide.

CIS Response:

"We agree with this recommendation. Conducting and reviewing PIAs require CIO as well as program office resources. Once the new PIA Guide and Template is approved and communicated, we will engage the DSO's so they can update their system privacy documentation. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-42)."

Recommendation 21

We recommend that each system owner annually review the existing PIA for their system to reevaluate current holdings of PII, and that they submit evidence of the review to CIS.

CIS Response:

"We agree with this recommendation. Conducting and reviewing PTAs/PIAs require CIO as well as program office resources. We plan on implementing a Privacy Threshold Analysis (PTA) process as part of our Privacy activities. The PTA is the initial step in determining whether a PIA is necessary and as indicated in NIST-800-122, an essential part of the Certification and Accreditation (C&A) process. The PTA will be reviewed annually or when a change occurs with the system and the document will become an artifact used for reporting purposes. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-43).

The Center for Information Services (CIS) security team has already began to share the evidence of annual PIA reviews with the Privacy Office to reflect that the DSO's are reviewing their PIA's as part of their FY09 security controls testing."

b) Compliance with privacy-related OMB Memoranda

OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, requires all federal agencies to develop and implement a "breach notification policy." The memorandum also outlines the privacy requirements related to the protection of PII, and reemphasizes the security requirements of OMB Memorandum M-06-16, Protection of Sensitive Agency Information. The following sections outline OPM's progress in implementing the requirements of these memoranda:

Implement a Breach Notification Process

OPM's Information Security and Privacy Policy Volume 2 contains limited instructions regarding breach notification procedures. However, the policy references the Incident Response and Reporting Guide, which contains a more detailed explanation of the internal and external entities that must be notified when a security breach occurs.

Review Current Holdings

In 2007, OPM's IT security officer issued a "PII Questionnaire" to the designated security officer for each of the Agency's major systems to determine whether the system contained PII. All new or significantly modified systems must complete an Initial Screening Assessment to determine if a PIA is required. However, as mentioned above, OPM's PIA process does not address all elements required by OMB, and system owners have not annually reviewed their PIAs to reevaluate current holdings of PII.

Reduce the Use of Social Security Numbers

OMB Memorandum M-07-16 required federal agencies to eliminate the use of social security numbers (SSNs) by the end of FY 2009. Although OPM has made progress in reducing the use of SSNs, the agency was unable to meet the timeline requirements of this memorandum.

In September 2009, CIS developed a formal plan to reduce the use of SSNs at OPM. The plan includes elements such as maintaining an inventory of OPM forms and validating the need for SSNs on these forms, working with system owners to scrub existing databases of SSNs, and providing guidance to system developers to mask SSN displays on reports and computer screens. However, the plan does not address participation in government-wide efforts to explore alternatives to agency use of SSNs, as required by OMB Memorandum M-07-16.

Recommendation 22 ***(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 12)***

We recommend that OPM continue its efforts to eliminate the unnecessary use of SSNs in accordance with OMB Memorandum M-07-16.

CIS Response:

"We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-12. However, the OCIO lacks the resources necessary to conduct the detailed analysis needed to review all documentation (laws, policies, OPM forms and other documents) that requires the use of SSNs today. Furthermore, those resources would be needed to establish and maintain the policies and procedures for an effective program."

Recommendation 23

We recommend that OPM participate in government-wide efforts to explore alternatives to agency use of SSNs, as required by OMB Memorandum M-07-16.

CIS Response:

"We agree with this recommendation."

Encryption

OMB Memorandum M-07-16 states that all data on mobile computers carrying sensitive data must be encrypted. CIS recently developed a new standard laptop image that utilizes software based full-disk encryption. We tested a sample laptop with this image and verified that the data on the device was secure.

CIS facilitates the purchase of all new laptops at OPM and ensures that an image with encryption capability is installed on each device. However, CIS was unable to provide evidence of how many laptops issued to OPM employees and contractors contain the new image with encryption capabilities.

Recommendation 24 ***(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 13)***

We recommend that CIS encrypt all data on all mobile computers containing sensitive information.

CIS Response:

"We agree with this recommendation. OPM has implemented mandatory encryption controls on OPM laptops, blackberries, and tape backups. OPM's IT Security and Privacy Policy requires that any sensitive data be removed to removable media must be encrypted. WinZip encryption has been provided to all OPM users to protect sensitive data. The encryption policy and guidelines for WinZip are available on the OPM intranet site and are included in the annual security awareness training. We are tracking this effort under CIS POAM FY09-Q1-CIS-13."

Control Remote Access

OPM has implemented a two-factor authentication requirement for controlling remote access to its information systems. In order to access OPM's internal applications remotely, users must connect to the OPM network through a Virtual Private Network (VPN) connection that requires both a personal identification number and a token number to authenticate.

Time-Out Function

OPM users remotely connected to the network through VPN must re-authenticate after 10 minutes of inactivity.

Log and Verify

In FY 2009, OPM developed a methodology for logging computer-readable data extracts of personally identifiable information (PII). The agency uses Team Track software to

track PII downloads and send an automatic notice to users 90 days after PII has been downloaded. When users receive this notification, they must either confirm PII data destruction or explain why the data has not been destroyed.

Incident Reporting and Handling Requirements

See section **IX**, Incident Reporting.

Rules and Consequences

OPM's IT Security and Privacy Policy Volume 2 outlines the consequences of violating OPM policies and procedures. The policy also outlines the penalties related to violations of the Privacy Act of 1974.

The recommendations outlined in this section indicate that OPM has not fully met the requirements of OMB Memoranda dating back to 2003. In addition, OPM's privacy group is currently undergoing an organizational realignment, and there is no permanent Privacy Program Manager in place. These conditions lead us to believe that there is a significant deficiency in OPM's management of its privacy program.

VIII. Configuration Management

This section details the controls OPM has in place regarding the technical configuration management of its major applications and user workstations.

a) Agency-wide security configuration policy

OPM has developed an agency-wide Security Configuration and Hardening Policy. This policy establishes standards for baseline configuration of the various operating platforms used by the agency and references build sheets for each platform that provide specific technical configuration guidance. OPM has also developed policies related to mainframe configuration integrity, configuration change control management, patch management, and system monitoring. However, the Security Configuration and Hardening Policy has not been updated since November 2004, and the patch management and system monitoring policies have not been updated since August 2005. See section **XII**, IT Security Policies and Procedures.

Recommendation 25

We recommend that OPM develop an up-to-date Security Configuration and Hardening Policy, Patch Management Policy, and System Monitoring Policy.

CIS Response:

"We agree with this recommendation. Some progress has been made in these procedures but currently the IT security group lacks the resources necessary to finalize and maintain these procedures. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We

have created CIS POA&Ms for each policy to track our progress (CIS POAM FY09-Q4-CIS-44, FY09-Q4-CIS-45, FY09-Q4-CIS-46)."

b) Techniques for monitoring compliance with policy

OPM uses [redacted] to routinely run scans of servers to ensure compliance with configuration guides. The agency also uses [redacted] to analyze individual workstations for compliance. Mainframe configuration compliance is monitored by [redacted], which [redacted] and produces detailed messages to warn of potential problems.

c) Federal Desktop Core Configuration

OPM has developed a Windows XP image that is generally compliant with Federal Desktop Core Configuration (FDCC) standards. There are eight settings in this image that do not meet FDCC compliance; OPM has documented justification for these deviations.

We conducted a test to verify that OPM's FDCC image is compliant with FDCC settings. OPM has implemented its FDCC compliant image on a test workstation in its LAN/WAN environment. We used [redacted]r to evaluate this workstation's compliance with FDCC settings; the results of the scan indicate that all settings on this workstation are FDCC compliant.

However, as of September 30, 2009, OPM's FDCC compliant image has not been implemented on any production workstations, and OPM has not documented and justified FDCC deviations for the standard image that is currently implemented on OPM workstations.

In addition, updated language from 48 CFR Part 39, Acquisition of Information Technology, has not been included in all contracts related to common security settings.

Recommendation 26 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 16)*

We recommend that OPM implement FDCC compliant images on all OPM workstations.

CIS Response:

"We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-16."

Recommendation 27

We recommend that OPM incorporate Federal Acquisition Regulation 2007-004 language in all contracts related to common security settings.

CIS Response:

"We agree with this recommendation. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-47)."

d) Follow-up on FY 2008 OIG [redacted] Recommendation

In the FY 2008 OIG FISMA audit report, we recommended that in the event that [redacted] cannot be remediated due to a technical or business reason, the supported system's owner should document the reason in the system's ISSP to formally accept any associated risks. In FY 2009, there remains one [redacted] vulnerability without a formally documented risk acceptance.

Recommendation 28 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 15)*

We recommend that in the event that an [redacted] vulnerability cannot be remediated due to a technical or business reason, the system's owner should document the reason in the system's ISSP and formally accept any associated risks.

CIS Response:

"We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-15."

IX. Incident Reporting

OPM has developed an "Incident Response and Reporting Policy" that outlines the responsibilities of OPM's Computer Incident Response Team (CIRT) and documents procedures for reporting all IT security events to the appropriate entities. We evaluated the degree to which OPM is following internal procedures and FISMA requirements for reporting security incidents internally, to the United States Computer Emergency Readiness Team (US-CERT), and to appropriate law enforcement authorities.

a) Identifying and reporting incidents internally

OPM's Incident Response and Reporting Policy requires the users of the agency's IT resources to immediately notify OPM's situation room when IT security incidents occur. During the past year, OPM has provided its employees with various forms of training related to the procedures to follow in the event sensitive data is lost. In addition, OPM reiterates the information provided in the Incident Response and Reporting Policy in the annual IT security and privacy awareness training.

OPM also notifies the OIG when security incidents occur by providing OIG investigators with a monthly report that tracks the security tickets related to the loss of sensitive data.

b) Reporting incidents to US-CERT

OPM's Incident Response and Reporting policy states that OPM's CIRT is responsible for sending incident reports to US-CERT on security incidents. OPM notifies US-CERT within one hour of a reportable security incident occurrence. Notification and ongoing correspondence with US-CERT is tracked through "security tickets" maintained by OPM's help desk.

c) Reporting incidents to law enforcement

The Incident Response and Reporting policy states that security incidents should also be reported to law enforcement authorities, where appropriate. Nothing came to the OIG's attention to indicate that this policy is not being followed.

X. Security Awareness Training

CIS has implemented a process to provide annual IT security and privacy awareness training to all OPM employees and contractors.

The training is conducted through an interactive web-based course. The course introduces employees and contractors to the basic concepts of IT security and privacy, including topics such as the importance of information security, security threats and vulnerabilities, viruses and malicious codes, privacy training, peer-to-peer software, and the roles and responsibilities of users.

Over 99 percent of OPM's employees and contractors completed the security awareness training course in FY 2009.

In addition, 99 percent of OPM employees and contractors with IT security-related responsibility completed specialized IT security training in FY 2009.

XI. E-authentication Risk Assessments

OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," states that it "applies to remote authentication of human users of Federal agency IT systems for the purposes of conducting government business electronically (or e-government)" and requires agencies to conduct an e-Authentication risk assessment of these systems.

OPM's system inventory identifies 10 systems that CIS believes are subject to e-Authentication requirements. However, we believe that there are at least five additional systems at OPM that are subject to e-Authentication requirements.

Recommendation 29

We recommend that CIS determine which systems in its inventory are subject to e-Authentication requirements and complete e-Authentication risk assessments for each of these systems.

CIS Response:

"We agree with this recommendation. After meeting with your office on August 24, 2009, the Center for Information Services (CIS) security team sent correspondence to the perspective DSO's that currently do not have an e-Authentication risk assessment but should have one. We are tracking this effort under CIS POAM FY09-Q1-CIS-48."

XII. IT Security Policies and Procedures

OPM's failure to adequately update its IT security policies and procedures has been highlighted in the past three OIG FISMA audit reports and has been identified as a material weakness in the IT security program in the FY 2007 and FY 2008 reports.

In FY 2009, OPM published a new Certification and Accreditation Guide and an Information Security and Privacy Policy and deleted the majority of the outdated information from the agency's internal website (THEO). However, the policies deleted from THEO have not been replaced with current guidance on managing IT security at OPM.

Volume 2 of the Information Security and Privacy Policy was posted to THEO in August 2009. This policy outlines the IT security controls that should be in place for the major applications owned by the agency. However, the majority of the text in this policy is derived or copied directly from NIST SP 800-53 and has not been tailored to specifically address OPM's IT environment. Although this policy assigns responsibility for the management of various controls, it does not provide guidance on how these controls should be implemented and monitored. OPM's DSO community has repeatedly voiced concern (directly to the OIG and to CIS at monthly IT security working group meetings) that the lack of detailed IT security policies and procedures has negatively impacted their ability to secure the information systems they manage.

The absence of the following policies, procedures, or guidance has directly led to OIG audit findings in FY 2009 (*this is not intended to be a comprehensive list of missing policies at OPM*):

- Procedures for DSOs to manage POA&Ms for agency systems;
- Procedures for CIS to review quarterly POA&Ms and report POA&M status to OMB;
- Guidance for developing contingency plans, procedures for routinely conducting contingency plan tests, and templates for reporting test results;
- Procedures for annually testing IT security controls and templates for recording test results;
- Policy and procedures related to oversight of systems operated by a contractor;
- Policy related to roles and responsibilities for the Independent Verification and Validation (IV&V) process and procedures for managing an IV&V; and
- Guidance for establishing agreements for interfacing systems.

In addition to the missing policies, the following OPM policies have not been updated in the past 3 years:

- Privacy Impact Assessment Guide (updated May 2006);
- Security Configuration and Hardening Policy (updated November 2004);
- Patch Management Policy (updated August 2005); and
- System Monitoring Policy (updated August 2005).

Although OPM has taken several steps to improve and update the agency's IT policies, we will continue to consider this condition a material weakness until adequate policies exist for all aspects of IT security program management at OPM. See section **I**, Information Security Governance.

Recommendation 30 ***(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 19)***

We recommend that CIS develop up-to-date and comprehensive IT security policies and procedures, and publish these documents to THEO.

CIS Response:

"We agree with this recommendation. With limited resources there was some progress made over the last 12 months in the creation of policies and procedures. However, the IT security group lacks the resources necessary to establish and maintain the IT security policies and procedures needed for an effective IT Security and Privacy program. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. This effort is being tracked under CIS POAM FY09-Q1-CIS-19."

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
- [redacted], Information Technology Auditor
- [redacted] Information Technology Auditor
- [redacted], Information Technology Auditor

Appendix I

Follow-up of Prior OIG FISMA Audit Recommendations

Report 4A-OD-00-05-013: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Enterprise Human Resources Integration (EHRI) Data Warehouse, issued May 9, 2005.

Rec #	Original Recommendation	Current Status
3	We recommend that the Office of e-Government Initiatives (e-Gov) implement independent organization segments for the development and migration of system programming changes to EHRI.	CLOSED

Report 4A-IS-00-05-026: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Electronic Questionnaire for Investigations Processing System (EQIP), issued June 16, 2005.

Rec #	Original Recommendation	Current Status
6	We recommend that each existing EQIP user (administrators, operators, and developers) sign a rules of behavior document. The signed documents should be maintained by the system DSO.	CLOSED
18	We recommend that the Federal Investigative Services Division (FISD) verify that only authorized users have access to EQIP and maintain authorization forms for users, including administrators, operators, and developers.	OPEN. FISD is currently updating OPM form 1665 to address this recommendation

Report 4A-IS-00-06-021: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Fingerprint Transaction System (FTS), issued August 29, 2006.

Rec #	Original Recommendation	Current Status
4	We recommend that FISD document and maintain on file authorizations that specify the authorized privileges for each FTS user. In addition, we recommend that FISD periodically verify that only authorized users have access to FTS by reviewing user authorization forms and comparing them to access lists.	CLOSED
7	We recommend that FISD update the FTS contingency plan to fully document the following information: • contact information, • recovery goals/objectives, • recovery procedures,	CLOSED

	• original or new site restoration procedures, • concurrent processing procedures, and • responsible teams.	

Report 4A-RI-00-08-023: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Employee Benefits Information System (EBIS), issued April 10, 2008.

Rec #	Original Recommendation	Current Status
1	We recommend that the Center for Human Capital Management Services (HCMS) develop a formal business impact analysis to determine the effect that EBIS system outages would have on HCMS, GRB, and EBIS users.	CLOSED
2	The EBIS contingency plan should be improved to include the appropriate elements outlined in NIST SP 800-34, as determined by the results of the business impact analysis.	CLOSED

Report 4A-WR-00-08-024: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Central Personnel Data File (CPDF), issued April 17, 2008.

Rec #	Original Recommendation	Current Status
1	We recommend that the Strategic Human Resources Policy Division update its Business Contingency Plan to include all elements required by NIST SP 800-34. This should include detailed recovery procedures sufficient to test the restoration of *all* CPDF processes.	CLOSED

Report 4A-HR-00-08-058: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's USAJOBS System, issued September 5, 2008.

Rec #	Original Recommendation	Current Status
1	We recommend that the Human Resources Products and Services Division (HRPS) and Monster World Wide (MWW) update, review, and test its contingency plan on an annual basis.	CLOSED
2	We recommend that HRPS/MWW develop formal procedures for media sanitization and disposal in accordance with NIST SP 800-53 Revision 1 control MP-6.	CLOSED
3	We recommend that HRPS update the most current POA&M template to identify and prioritize all security weaknesses identified for USAJOBS.	CLOSED

Report 4A-MO-00-08-059: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Executive Schedule C System (ESCS), issued September 8, 2008.

Rec #	Original Recommendation	Current Status
1	We recommend that the Human Capital Leadership & Merit System Accountability Division (HCLMSA) update the ESCS contingency plan to include the elements outlined above as suggested by NIST SP 800-34.	CLOSED
3	We recommend that the [redacted] supporting ESCS be updated with [redacted] in a timely manner.	CLOSED
4	We recommend that HCLMSA update the ESCS POA&M to include the weaknesses outlined in this audit report, and continue to update the POA&M with any additional weaknesses discovered by the program office or an outside party conducting a security review of the system.	CLOSED

Report 4A-CI-00-08-022: FY 2008 Federal Information Security Management Act Audit, issued September 23, 2008.

Rec #	Original Recommendation	Current Status
1	We recommend that OPM ensure that an annual test of security controls has been completed for all systems.	OPEN. Rolled forward as 4A-CI-00-09-031 Recommendation 6
2	We recommend that OPM's program offices test the contingency plans for each system on an annual basis.	OPEN. Rolled forward as 4A-CI-00-09-031 Recommendation 9
3	We recommend that OPM update its system inventory to clearly identify the state of the system (active, suspended, development, etc).	CLOSED
4	We recommend that the program offices incorporate all known security weaknesses into the POA&Ms.	OPEN. Rolled forward as 4A-CI-00-09-031 Recommendation 12
5	We recommend that an up-to-date POA&M exist for each system in OPM's inventory.	OPEN. Rolled forward as 4A-CI-00-09-031 Recommendation 13
6	We recommend that all program offices submit POA&Ms to the CIS/CIO office on a quarterly basis.	OPEN. Rolled forward as 4A-CI-00-09-031 Recommendation 13
7	We recommend that the CIS/CIO require each program office to provide evidence (proof of closure) that POA&M weaknesses have been resolved before allowing that item to be labeled "complete."	CLOSED

8	We recommend that all OIG recommendations be included on POA&Ms and they not be removed until evidence of proof of closure is provided to the CIS/CIO.	CLOSED
9	We recommend that CIS take the appropriate steps to ensure that all active systems in OPM's inventory have a complete and current C&A.	OPEN. Rolled forward as 4A-CI-00-09-031 Recommendation 16
10	We recommend that all elements required by FISMA and relevant NIST guidance be in place before a system is formally C&A'd.	CLOSED
11	We recommend that OPM issue its "Information Security and Privacy Policy" to all agency employees and post a copy to the agency's internal website.	CLOSED
12	We recommend that OPM continue its efforts to reduce the use of SSNs and develop a formal plan to eliminate the unnecessary collection and use of SSNs within 18 months in accordance with OMB Memorandum M-07-16.	OPEN. Rolled forward as 4A-CI-00-09-031 Recommendation 22
13	We recommend that OPM continue its efforts to implement a solution to automatically encrypt all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive.	OPEN. Rolled forward as 4A-CI-00-09-031 Recommendation 24
14	We recommend that OPM continue its efforts to develop a methodology for logging computer-readable data extracts to determine whether sensitive data has been erased after 90 days.	CLOSED
15	We recommend that OPM configure its [redacted] in a manner consistent with OPM's [redacted] Configuration Policy. Each of the vulnerabilities outlined in the OIG's audit inquiry should be formally documented, itemized, and prioritized in a POA&M. In the event that a vulnerability cannot be remediated due to a technical or business reason, the supported system's owner should document the reason in the system's ISSP to formally accept any associated risks.	OPEN. Rolled forward as 4A-CI-00-09-031 Recommendation 28
16	We recommend that OPM continue its efforts to implement all required elements of the FDCC.	OPEN. Rolled forward as 4A-CI-00-09-031 Recommendation 26
17	We recommend that OPM continue its efforts to ensure that all federal employees and contractors with access to OPM's IT resources complete IT security and privacy awareness training on an annual basis.	CLOSED
18	We recommend that e-authentication risk assessments be completed for the required systems in accordance with OMB Memorandum M-04-04.	CLOSED

19	We recommend that CIS promptly update OPM's IT security policies and publish them to THEO.	OPEN. Rolled forward as 4A-CI-00-09-031 Recommendation 30

Report 4A-CI-00-09-053: Flash Audit Alert – Information Technology Security Program at the U.S. Office of Personnel Management, issued May 27, 2009.

Rec #	Original Recommendation	Current Status
1	We recommend that CIS correct the FY 2009 second quarter FISMA report to accurately reflect the status of OPM's IT security position as of March 1, 2009.	CLOSED
2	We recommend that CIS develop a comprehensive set of IT security policies and procedures, and a plan for updating it at least annually.	OPEN. Rolled forward as 4A-CI-00-09-031 Recommendation 30
3	We recommend that the OPM Director ensure that CIS has adequate resources to properly staff its IT Security and Privacy Group.	OPEN
4	We recommend that CIS recruit a permanent Senior Agency Information Security Officer as soon as possible and adequate staff to effectively manage the agency's IT security program.	OPEN. OPM hired an ITSO, but the organization of the ITSO's staff has not been finalized.

Appendix II

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Management Services
Division

MEMORANDUM FOR PATRICK E. McFARLAND
Inspector General

JUL 28 2009

FROM: JANET L. BARNES
Chief Information Officer

SUBJECT: Response to OIG IT Security Flash Audit Alert

The OPM Office of Inspector General (OIG) released a Flash Audit Alert dated May 27th, 2009, which outlined several recommendations regarding the OPM IT Security Program. These recommendations are noted below along with our response.

Recommendation 1: We recommend that CIS correct the FY 2009 second quarter FISMA report to accurately reflect the status of OPM's IT security position as of March 1, 2009. This would include reporting that eOPF and the EHRI Data Warehouse systems both have weaknesses more than 120 days overdue, and changing the metrics on the entire report from the number of overdue weaknesses to the number of systems with overdue weaknesses.

Response: The Center for Information Services (CIS) security team acted on the best information they had at the time in closing eOPF and EHRI Data Warehouse weaknesses. In response to the concern raised by OIG staff that 21 were closed inappropriately – out of a total of 268 total program weaknesses - CIS considered the OIG rationale for why these 21 should remain open (the guidance on this is not clear) and agreed to re-open them. They have been re-opened with the original targeted completion date. OIG was advised of this action prior to Alert Report.

2009 JUL 28 PM 5:20

We agree with the recommendation that OPM report the number of systems with weaknesses more than 120 days overdue, instead of the number of weaknesses. This was a mistake in our understanding of the reporting requirement. It should be noted that this mistake made the OPM metrics look worse than they really were – so we were most willing to make this change. As soon as we confirmed the OIG's observation was correct, we made the change, in time for the 3rd quarter FISMA report. OIG was notified of the correction prior to the Alert Report. The 2nd quarter report has also been updated and sent to OMB. We consider this recommendation to be closed.

Recommendation 2: We recommend that CIS develop a comprehensive set of IT security policies and procedures, and a plan for updating them at least annually.

Response: We agree with this recommendation and have been working for many months to complete needed updates. Work began as soon as funding was provided. Many policies and procedures have already been revised, with the remainder targeted for completion by 8/31/09. We have kept OIG apprised of our efforts to complete this work.

Recommendation 3: We recommend that the OPM Director ensure that CIS has adequate resources to properly staff its IT Security and Privacy Group.

Response: We agree with this recommendation. As we discussed with OIG staff on numerous occasions, CIS has been working with HR for more than a year to reorganize and elevate the IT security function, to upgrade the level of the IT security officer from a GS-14 to a GS-15, and to add staff. A new organizational alignment, grade structure and resources for the IT Security and Privacy Group were approved on March 4, 2009. Under this new structure, the IT security staff will grow from 3 to 6. We consider this recommendation to be closed.

Recommendation 4: We recommend that CIS recruit a permanent Senior Agency Information Security Officer as soon as possible, and adequate staff to effectively manage the agency's IT security program.

Response: We agree with this recommendation. Recruiting has been in progress since the reorganization was approved. We have made a couple of offers to fill the GS-15 and GS-14 positions, which were declined. We have identified another excellent candidate for the Gs-15 position. We are currently in the process of getting Chief of Staff approval to extend an offer. We are targeting a report date in August.

As you can see, all of the OIG issues with our security program noted in the Alert Report have either been completed or are well on their way to completion. With the exception of the selection of the ITSO, which is a very recent decision, we have attempted to keep OIG staff apprised of our status on these issues. Their recommendations were seriously considered, reviewed and acted upon as appropriate.

Appendix III

October 20, 2009

Report No. 4A-CI-00-09-031

MEMORANDUM FOR LEWIS F. PARKER, Jr.
Chief, Information Systems Audit Group

FROM: [redacted]
Acting Chief Information Officer

SUBJECT: Federal Information Security Management Act Audit – FY 2009

Attached you will find our responses to the **draft** Federal Information Security Management Act audit report. The protection of the Office of Personnel Management (OPM) network and resources is critical to the success of the OPM mission. All OPM Components rely extensively on information technology (IT) assets and the OPM network to achieve mission objectives. For that reason, we thank you and agree with the recommendations provided in the draft report identifying areas for improvement within the OPM IT security and privacy program. The Office of the Chief Information Officer (OCIO) is committed to ensuring an effective IT security and privacy program. Please note that we have created CIO POA&M entries for these findings and will develop a plan to mitigate these as additional resources become available.

If you have any questions regarding the responses in this report, please don't hesitate to contact me at [redacted] or [redacted] (ITSO) at [redacted]. We look forward to continue to work together to improve the IT security and privacy program at OPM.

Attachment

cc: [redacted]
Chief of staff and Director of External Affairs

[redacted]
Deputy Chief Financial Officer & Policy and Internal Control Group

[redacted]
Deputy Chief of Staff and Executive Secretariat

Current Status of Flash Audit Alert Recommendation 1

We verified that CIS corrected and submitted the FY 2009 second quarter FISMA report. We also verified that the FY 2009 third quarter FISMA report accurately represented the status of OPM's security program at that time.

CIS Reply 10/20/09

The Center for Information Services (CIS) security team will continue to ensure the quarterly FISMA reports reflect correct and accurate information for OPM's security program.

Current Status of Flash Audit Alert Recommendation 2

OPM's IT security policies and procedures continue to lack adequate current guidance on managing IT security at the agency. See section **XII** of this report for details.

CIS Reply 10/20/09

Please refer to section XII for our response to Recommendation 30 regarding the IT security policies and procedures.

Current Status of Flash Audit Alert Recommendation 3

We continue to believe that CIS lacks the resources needed to manage an adequate IT security program. Eleven of the nineteen audit recommendations issued in the FY 2008 FISMA audit report have been rolled forward into this FY 2009 FISMA report, indicating that CIS does not have the resources needed to remediate identified security weaknesses.

CIS Reply 10/20/09

We agree with this recommendation. Currently the IT security group lacks the resources necessary to establish and maintain an effective security and privacy program. The new SAISO (referred to as the ITSO) that was hired in September 2009 has identified resources needed and his recommendations are under review with senior management. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-27).

Current Status of Flash Audit Alert Recommendation 4

CIS hired a permanent SAISO (referred to as the ITSO) in September 2009. However, the agency operated with an acting ITSO for over 11 months of FY 2009. In addition, the organization of the staff reporting to the ITSO has not been finalized. On a potentially positive note, the OPM Director has recently appointed a new Acting Chief Information Officer, who has developed preliminary plans to expand and improve OPM's IT security program. We will re-evaluate these developments during the FY 2010 FISMA audit.

CIS Reply 10/20/09

We agree with this recommendation. Currently the IT security group lacks the resources and the organizational structure necessary to establish and maintain an effective security and privacy program. The new SAISO (referred to as the ITSO) that was hired in September 2009

has developed an organizational chart, roles and responsibilities and resources needed. His recommendations are under review with senior management. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. As referenced in Flash Audit Alert Recommendation 3, we have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-27) regarding resources.

Recommendation 1

We recommend that CIS conduct a survey of OPM program offices (particularly the Benefits Systems Group) to identify any systems that exist but do not appear on the system inventory. The systems discovered during this survey should be promptly added to the system inventory and certified and accredited.

CIS Reply 10/20/09

We agree with this recommendation. The IT Security and Privacy group will conduct a network assessment to map out the OPM network and identify all missing systems and created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-28).

Recommendation 2

We recommend that CIS develop and maintain an inventory of all system interfaces.

CIS Reply 10/20/09

We agree with this recommendation. The IT Security and Privacy team will include system interface information on the OPM FISMA Master System Inventory going forward. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-29). Please note as stated in response to IG Information Request #24, system interface information is included within each System Security Plan for each system currently on the OPM FISMA Master System Inventory.

Recommendation 3

We recommend that CIS develop a policy providing guidance on the development and appropriate use of MOUs and ISAs.

CIS Reply 10/20/09

We agree with this recommendation. Currently the IT Security and Privacy group lacks the resources necessary to establish and maintain an effective security and privacy program. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-30).

Recommendation 4

We recommend that CIS conduct a survey to determine how many systems owned by another agency are used by OPM.

CIS Reply 10/20/09

We agree with this recommendation. We have made some progress with this task (please refer to IG Information request #24) but we lack the resources to conduct a complete network assessment to map out the OPM network and identify all systems. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-31).

Recommendation 5

We recommend that CIS develop a policy for adequately testing the security controls of OPM's systems, and provide training to the Designated Security Officer (DSO) community related to proper security control testing.

CIS Reply 10/20/09

We agree with this recommendation. Currently the IT security group lacks the resources necessary to establish and maintain these policies and training program. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-32).

Recommendation 6 ***(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 1)***

We recommend that OPM ensure that an annual test of security controls has been completed for all systems.

CIS Reply 10/20/09

We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-1.

Recommendation 7

We recommend that OPM develop detailed guidance related to developing and testing the contingency plans of agency systems, and provide training to the DSO community related to proper contingency planning and contingency plan testing.

CIS Reply 10/20/09

We agree with this recommendation. Currently the IT security group lacks the resources necessary to establish and maintain these policies and training program. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-33).

Recommendation 8

We recommend that up-to-date contingency plans be developed for all agency systems.

CIS Reply 10/20/09

We agree with this recommendation. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-34).

Recommendation 9 (*Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 2)*
We recommend that OPM's program offices test the contingency plans for each system on an annual basis.

CIS Reply 10/20/09
We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-2.

Recommendation 10
We recommend that OM develop a policy providing guidance on providing adequate oversight of contractor operated systems.

CIS Reply 10/20/09
We agree with this recommendation. Currently the IT security group lacks the resources necessary to establish and maintain these policies and provide the oversight needed. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-35).

Recommendation 11
We recommend that CIS publish the Plan of Action and Milestone Standard Operating Procedure to THEO.

CIS Reply 10/20/09
We agree with this recommendation. We have created a CIS POA&M item to document the completion of this recommendation (CIS POAM FY09-Q4-CIS-36). The POA&M Guide has been published as of September 2009 on Theo - http://theo.opm.gov/policies/ispp/FINAL_POAM_Process_SOP_093009.pdf

Recommendation 12 (*Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 4)*
We recommend that OPM program offices incorporate all known IT security weaknesses into POA&Ms.

CIS Reply 10/20/09
We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-4. Since the POA&M SOP was just recently published on Theo, we will continue to assist program offices through this process.

Recommendation 13 (*Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendations 5 and 6)*
We recommend that an up-to-date POA&M exist for each system in OPM's inventory, and that system owners submit updated POA&Ms to CIS on a quarterly basis.

CIS Reply 10/20/09
We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-5 and CIS POAM FY09-Q1-CIS-6. The POA&M SOP has been published as of September 2009 which provides guidance to DSO's regarding POA&M submission. Please

note that since OMB did not require any POA&M submissions for FY09 quarter 4, CIS did not continue to follow up with program offices to ensure submissions were provided to CIS for FY09 quarter 4.

Recommendation 14
We recommend that CIS provide guidance to program offices to evaluate the resources and time requirements needed to remediate security weaknesses so that reasonable remediation due dates are established for all POA&M items.

CIS Reply 10/20/09
We agree with this recommendation. The POA&M SOP has been published as of September 2009 which provides guidance to DSO's regarding POA&M management. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-37) on supplemental guidance to the DSO's.

Recommendation 15
We recommend that each program office prioritize the system weaknesses listed on their POA&Ms.

CIS Reply 10/20/09
We agree with this recommendation. The POA&M SOP has been published as of September 2009 which provides guidance to DSO's regarding prioritizing weaknesses. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-38) on supplemental guidance to the DSO's.

Recommendation 16 ***(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 9)***
We recommend that all active systems in OPM's inventory have a complete and current C&A.

CIS Reply 10/20/09
We agree with this recommendation. The IT Security and Privacy group would like to conduct a network assessment to map out the OPM network and identify all systems and account for missing C and A's but we currently lack the resources to perform this task. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We are tracking this effort under CIS POAM FY09-Q1-CIS-9.

Recommendation 17
We recommend that the FIPS Publication 199 security categorization be updated for the inappropriately categorized system.

CIS Reply 10/20/09
We agree with this recommendation. The Center for Information Services (CIS) security team will work with the DSO's to ensure the FIPS 199 reflect the appropriate rating. During the monthly October 2009 Information Technology Security Working Group (ITSWG) meeting, the writer and subject matter expert from NIST provided a briefing on NIST 800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories) to the DSO's and CIS. We have created a CIS POA&M item to continue to track our progress (CIS POAM FY09-Q4-CIS-39).

Recommendation 18
We recommend that CIS update the PIA Guide to address all of the requirements of OMB Memorandum M-03-22.

CIS Reply 10/20/09
We agree with this recommendation. The privacy group is currently working on a new PIA Guide and a new PIA Template. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-40).

Recommendation 19
We recommend that CIS conduct a new PIA survey to determine which OPM systems require a PIA, including those systems that process sensitive information about government employees and contractors.

CIS Reply 10/20/09
We agree with this recommendation. The IT Security and Privacy group would like to conduct a network assessment to identify all PII information present on the OPM network but we currently lack the resources to perform this task. The network assessment would be followed by a request to each office that owns the PII to conduct privacy threshold analysis (PTA). The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-41).

Recommendation 20
We recommend that a new PIA be conducted for the appropriate systems based on the updated PIA Guide.

CIS Reply 10/20/09
We agree with this recommendation. Conducting and reviewing PIAs require CIO as well as program office resources. Once the new PIA Guide and Template is approved and communicated, we will engage the DSO's so they can update their system privacy documentation. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-42).

Recommendation 21
We recommend that each system owner annually review the existing PIA for their system to reevaluate current holdings of PII, and that they submit evidence of the review to CIS.

CIS Reply 10/20/09
We agree with this recommendation. Conducting and reviewing PTAs/PIAs require CIO as well as program office resources. We plan on implementing a Privacy Threshold Analysis (PTA) process as part of our Privacy activities. The PTA is the initial step in determining whether a PIA is necessary and as indicated in NIST-800-122, an essential part of the Certification and Accreditation (C&A) process. The PTA will be reviewed annually or when a change occurs with the system and the document will become an artifact used for reporting purposes. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-43).

The Center for Information Services (CIS) security team has already began to share the evidence of annual PIA reviews with the Privacy Office to reflect that the DSO's are reviewing their PIA's as part of their FY09 security controls testing.

Recommendation 22 ***(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 12)***
We recommend that OPM continue its efforts to eliminate the unnecessary use of SSNs accordance with OMB Memorandum M-07-16.

CIS Reply 10/20/09
We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-12. However, the OCIO lacks the resources necessary to conduct the detailed analysis needed to review all documentation (laws, policies, OPM forms and other documents) that requires the use of SSNs today. Furthermore, those resources would be needed to establish and maintain the policies and procedures for an effective program.

Recommendation 23
We recommend that OPM participate in government-wide efforts to explore alternatives to agency use of SSNs, as required by OMB Memorandum M-07-16.

CIS Reply 10/20/09
We agree with this recommendation.

Recommendation 24 ***(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 13)***
We recommend that CIS encrypt all data on all mobile computers containing sensitive information.

CIS Reply 10/20/09
We agree with this recommendation. OPM has implemented mandatory encryption controls on OPM laptops, blackberries, and tape backups. OPM's IT Security and Privacy Policy requires that any sensitive data be removed to removable media must be encrypted. WinZip encryption has been provided to all OPM users to protect sensitive data. The encryption policy and guidelines for WinZip are available on the OPM intranet site and are included in the annual security awareness training. We are tracking this effort under CIS POAM FY09-Q1-CIS-13.

Recommendation 25

We recommend that OPM develop an up-to-date Security Configuration and Hardening Policy, Patch Management Policy, and System Monitoring Policy.

CIS Reply 10/20/09

We agree with this recommendation. Some progress has been made in these procedures but currently the IT security group lacks the resources necessary to finalize and maintain these procedures. The Office of the Chief Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. We have created CIS POA&Ms for each policy to track our progress (CIS POAM FY09-Q4-CIS-44, FY09-Q4-CIS-45, FY09-Q4-CIS-46).

Recommendation 26 ***(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 16)***

We recommend that OPM implement FDCC compliant images on all OPM workstations.

CIS Reply 10/20/09

We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-16.

Recommendation 27

We recommend that OPM incorporate Federal Acquisition Regulation 2007-004 language in all contracts related to common security settings.

CIS Reply 10/20/09

We agree with this recommendation. We have created a CIS POA&M item to track our progress (CIS POAM FY09-Q4-CIS-47).

Recommendation 28 ***(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 15)***

We recommend that in the event that an [redacted] cannot be remediated due to a technical or business reason, the system's owner should document the reason in the system's ISSP and formally accept any associated risks.

CIS Reply 10/20/09

We agree with this recommendation. We are tracking this effort under CIS POAM FY09-Q1-CIS-15.

Recommendation 29

We recommend that CIS determine which systems in its inventory are subject to e-Authentication requirements and complete e-Authentication risk assessments for each of these systems.

CIS Reply 10/20/09

We agree with this recommendation. After meeting with your office on August 24, 2009, the Center for Information Services (CIS) security team sent correspondence to the perspective DSO's that currently do not have an e-Authentication risk assessment but should have one. We are tracking this effort under CIS POAM FY09-Q1-CIS-48.

Recommendation 30 ***(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 19)***

We recommend that CIS develop up-to-date and comprehensive IT security policies and procedures, and publish these documents to THEO.

CIS Reply 10/20/09

We agree with this recommendation. With limited resources there was some progress made over the last 12 months in the creation of policies and procedures. However, the IT security group lacks the resources necessary to establish and maintain the IT security policies and procedures needed for an effective IT Security and Privacy program. The Office of the Chief

Information Officer (OCIO) is working on acquiring resources needed for the IT Security and Privacy program. This effort is being tracked under CIS POAM FY09-Q1-CIS-19.