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 2011

Report No. 4A-CI-00-11-009

Date: November 9, 2011

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 2011

WASHINGTON, D.C.

Report No. 4A-CI-00-11-009

Date: November 9, 2011

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 2011

WASHINGTON, D.C.

Report No. 4A-CI-00-11-009

Date: November 9, 2011

This audit report documents the Office of Personnel Management's (OPM's) continued efforts to manage and secure its information resources. We have significant ongoing concerns regarding the overall quality of the information security program at OPM.

In fiscal year (FY) 2007 and FY 2008, we reported a material weakness in controls over the development and maintenance of OPM's information technology (IT) security policies. In FY 2009, we issued a Flash Audit Alert to OPM's Director highlighting our concerns with the agency's IT security program. We also expanded the material weakness related to IT security policies to include concerns with the agency's overall information security governance and its information security management structure. This material weakness was rolled forward through FY 2010.

In FY 2011, OPM's Office of the Chief Information Officer (OCIO) made progress in updating its IT security and privacy policies, procedures, and guidance. However, the OCIO continues to operate with a decentralized IT security structure and does not have the authority or the resources available to adequately implement the new policies. We continue to believe that information security governance represents a material weakness in OPM's IT security program.

In FY 2010, we added a second material weakness related to the management of the Certification and Accreditation (C&A) process. We reported that there were, in our opinion, three root causes of OPM's C&A issues: insufficient staffing in the IT Security and Privacy Group, a lack of policy and procedures, and the decentralized DSO model in place at OPM.

In FY 2011, the OCIO improved the policy deficiencies by publishing updated procedures and templates designed to improve the overall C&A process (now referred to as Security Assessment and Authorization or Authorization process) and dedicating resources to facilitating the Authorization process. We observed an improvement in the Authorization packages completed under this new process, and believe that this improvement warrants reducing the material weakness related to C&As to a significant deficiency. Although no longer a material weakness, the Authorization process continues to be hindered by limited OCIO staffing resources and the decentralized DSO model.

In addition to the material weaknesses described above, we noted the following controls in place and opportunities for improvement:

- The OCIO has implemented risk management procedures at a system-specific level, but has not developed an agency-wide risk management methodology.
- The IT security controls were adequately tested for only 36 of 48 information systems in OPM's inventory.
- The OCIO has implemented an agency-wide information system configuration management policy and has established configuration baselines for all operating platforms used by the agency.
- The OCIO routinely conducts vulnerability scans of production servers, but does not have a formal process for tracking the status of weaknesses identified through the scanning.
- The OCIO has developed thorough incident response and reporting capabilities.
- The OCIO has implemented a process to provide annual IT security and privacy awareness training to all OPM employees and contractors. However, controls related to providing specialized security training to individuals with information security responsibility could be improved.
- Plans of Action and Milestones are appropriately managed for all information systems in OPM's inventory. The OCIO has the capability to use two-factor authentication for remote access, but this control was not enforced for all users in FY 2011.
- We found that several OPM employees maintained network access after their termination date, and several users had multiple accounts.
- The OCIO has taken steps toward implementing a continuous monitoring program at OPM; however, this project remains a work in progress.
- The OCIO developed a catalog of information security controls that are shared ("common") with all of the agency's applications. However, the current version of the catalog is incomplete, as it does not account for the large number of technical controls that are common to applications residing on one of OPM's several general support systems. As a result, the

owner of each application residing on a support system must independently test the same controls.

- The contingency plans were adequately tested for only 40 of 48 information systems in OPM's inventory.
- We noticed inconsistency in the quality of contingency plan testing documentation produced for various OPM systems. In September 2011, the OCIO issued detailed guidance to program offices on how to conduct a contingency plan test and create an after action report. As part of the FY 2012 FISMA audit, we will test the impact that this new guidance has on the quality of system level contingency plan tests.
- Contingency plan/disaster recovery tests are not coordinated between OPM's various general support systems.
- OPM program offices appeared to provide an adequate level of oversight to contractor-operated systems. However, the techniques and quality of this oversight was inconsistent between program offices.
- OPM maintains an adequate security capital planning and investment program for information security.

Contents

Page

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 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 strategic, agency-wide security responsibility. At OPM, security responsibility is assigned to the agency's Office of the Chief Information Officer (OCIO). 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 its control.

To assist agencies and IGs in fulfilling their FISMA evaluation and reporting responsibilities, the Department of Homeland Security (DHS) National Cyber Security Division issued the fiscal year (FY) 2011 Inspector General FISMA Reporting Instructions. This document provides a consistent form and format for agencies to report to DHS. It identifies a series of reporting topics that relate to specific agency responsibilities outlined in FISMA. Our audit and reporting strategies were designed in accordance with the above DHS guidance.

Objectives

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

- Risk Management;
- Security Configuration Management;
- Incident Response and Reporting Program;
- Security Training Program;
- Plans of Action and Milestones (POA&M) Program;
- Remote Access Program;
- Identity and Access Management;
- Continuous Monitoring Program;
- Contingency Planning Program;

- Agency Program to Oversee Contractor Systems; and,
- Agency Security Capital Planning Program.

In addition, we evaluated the status of OPM's IT security governance structure and its Security Assessment and Authorization process. These two areas represented material weaknesses in OPM's IT security program in prior FISMA audits.

We also evaluated the security controls of four 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

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit covered OPM's FISMA compliance efforts throughout FY 2011.

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

- Enterprise Server Infrastructure General Support System (OIG Report No. 4A-CI-00-11-016);
- Consolidated Business Information System (OIG Report No. 4A-CF-00-11-015);
- Presidential Management Fellows System (OIG Report No. 4A-HR-00-11-017); and,
- Center for Talent Services General Support System (OIG Report No. 4A-CI-00-11-043).

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. Accordingly, we obtained an understanding of the internal controls for these various systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of these systems' internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented. As appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

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.

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 for these various systems taken as a whole.

The criteria used in conducting this audit include:

- DHS National Cyber Security Division FY 2011 Inspector General Federal Information Security Management Act Reporting Instructions;
- OPM Information Technology Security and Privacy Policy Handbook;
- OPM Information Technology Security FISMA Procedures;
- OPM Security Assessment and Authorization Guide;
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- 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 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems;
- NIST SP 800-39, Managing Information Security Risk;
- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems;
- NIST SP 800-60 Version 2.0 Volume II, 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; 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 2011 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 OCIO 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 our FY 2011 FISMA audit of OPM's IT Security Program. Several recommendations were issued in FY 2010 and are rolled forward from OIG report no. 4A-CI-00-10-019, "Federal Information Security Management Act Audit – FY 2010."

I. Information Security Governance

Over the past fiscal year OPM's OCIO has made progress in updating its IT security and privacy policies, procedures, and guidance. However, the existence of policies alone cannot improve the agency's IT security program. The OCIO continues to operate with a decentralized IT security structure and does not have the resources available to adequately implement the new policies. We continue to believe that information security governance represents a material weakness in OPM's IT security program.

The sections below outline the OIG's review of IT security governance at OPM.

a) IT Security Policies and Procedures

OPM's failure to adequately update its IT security and privacy policies and procedures was highlighted in the past five annual OIG FISMA audit reports, and was identified as a material weakness in the agency's IT security program in the past four FISMA audit reports.

In FY 2011, the OCIO created and published several new documents that provide a policy framework for OPM's IT security program, including:

- Information Security and Privacy Policy Handbook (March 2011);
- Information Technology Security FISMA Procedures (May 2011); and,
- OPM Security Assessment and Authorization Guide (April 2011).

These three documents address many of the policies and procedures that we had identified as missing or inadequate in prior FISMA audits. However, the creation of policies and procedures alone does not improve an IT security program. They must be fully adopted by the target audience, in this case the Designated Security Officer (DSO) community. Given the decentralized structure of OPM's IT security program, it is questionable whether the DSOs have the skills and resources necessary to implement the new policies and procedures.

The quantity of IT security deficiencies outlined in this audit report indicate that, despite the existence of policies, limited improvement has been made in the overall security program to date. It remains to be seen whether the new policy and procedure framework will lead to notable improvements in the future.

While the majority of missing policies and procedures have now been created, we identified several specific areas where OPM continues to lack adequate IT policies, procedures, or guidance, including:

- Policy and procedures related to oversight of systems operated by a contractor;
- Policy on agency-wide risk management (see Recommendation 5);
- Policy related to roles and responsibilities for the Independent Verification and Validation (IV&V) process and procedures for managing an IV&V; and,
- Policy or guidance for identifying and continuously monitoring high risk security controls.

Recommendation 1

We recommend that the OCIO develop policies to address oversight of contractor systems, agency-wide risk management, IV&V, and continuous monitoring of high risk security controls.

OCIO Response:

"The CIO partially concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The policies in the IT Security Handbook dated March 31, 2011 apply to all OPM systems including those at contractor facilities and therefore a new policy for oversight of contractor systems is not necessary. The CIO believes that new policies for IV&V and continuous monitoring of high risk security controls should be developed and would be beneficial to the OPM security program."

OIG Reply:

Although OPM's IT Security Handbook may apply to contractors, we determined that the techniques and quality of oversight provided to contractor systems was inconsistent between program offices. This inconsistency is the result of OPM not having an agency-wide policy providing program offices guidance on overseeing the activities of contractors operating OPM systems. We continue to recommend that the OCIO develop policies to address oversight of contractor systems, IV&V, and continuous monitoring of high risk security controls.

b) Information Security Management Structure

The FY 2010 FISMA report highlighted the fact that OPM had operated without a permanent Senior Agency Information Security Officer (SAISO) for over 18 months and that the SAISO's Information Technology Security and Privacy Group (ITSPG) did not have the resources necessary to adequately manage OPM's IT security program.

The OCIO had a permanent SAISO throughout FY 2011 and also hired several new employees and contractors to work in the ITSPG. However, the quantity and variety of audit recommendations throughout this report indicates that the OCIO continues to lack the resources necessary to remediate long standing IT security weaknesses and fully implement the recently developed policies and procedures. In addition, 18 audit recommendations from FY 2010 were not adequately addressed in FY 2011. We believe that a major factor contributing to these problems is the OCIO's lack of direct

authority over the DSO community tasked with managing the security of OPM's major information systems.

OPM chose to implement a decentralized model in which the DSOs are typically appointed by and report to the program offices that own major computer systems. Very few of the DSOs have any background in information security, and most are only managing their security responsibilities as a collateral duty to their primary job function. The OCIO continues to provide guidance to the DSO community through monthly Information Technology Security Working Group (ITSWG) meetings. However, these meetings provide limited benefit because 1) the OCIO has no authority over the DSOs and cannot mandate their attendance at the ITSWG meetings, and 2) not all DSOs have the technological skills or the resources required to implement the security concepts discussed at these meetings.

Several sections of this report exemplify the impact of the OCIO's lack of authority over DSOs, including:

- The IT security controls of only 36 of 48 systems in OPM's inventory were adequately tested in FY 2011 by the program offices owning the system (see section III, below).
- The contingency plans were adequately tested for only 40 of 48 systems in OPM's inventory (see section XI, below). Of the contingency plans that were tested, the quality varied greatly between tests conducted by various program offices.
- Only 75% of personnel that the OCIO identified as having significant IT security responsibility received adequate training in FY 2011 (see section VI, below).

IT security is a shared responsibility between the OCIO and program offices. The OCIO is responsible for overall information security governance while program offices are responsible for the security of the systems that they own. There is a balance that must be maintained between a consolidated and a distributed approach to managing IT security. It is still our opinion that OPM's approach is too decentralized. OPM program offices should continue to be responsible for maintaining security of the systems that they own, but the DSO responsibility for documenting, testing, and monitoring system security should be centralized within the OCIO.

Recommendation 2 (*Rolled-Forward from 2010)*

We recommend that OPM implement a centralized information security governance structure where all information security practitioners, including designated security officers, report to the SAISO. Adequate resources should be assigned to the OCIO to create this structure. Existing designated security officers who report to their program offices should return to their program office duties. The new staff that reports to the SAISO should consist of experienced information security professionals.

OCIO Response:

"The CIO concurs with this recommendation and offers the following remarks. The CIO's budget does not contain funding to replace the Designated Security Officers with information security professionals. One possible suggestion is to require OPM program offices to provide funding for the CIO to hire information security professionals."

OIG Reply:

We acknowledge the fact that the OCIO does not currently have funding to hire enough security professionals to manage all of OPM's information systems. Migrating OPM to a more centralized IT security function will require the cooperation of the program offices that own the agency's major applications. The OCIO should seek the assistance of the OPM Director in negotiating with program offices to transfer responsibility of some security functions to a centralized group reporting to the CIO. Although this initiative will take an extended amount of time, the OCIO should begin working with the owners of applications it determines to be high risk, such as financial systems and applications containing large amounts of sensitive data.

II. Security Assessment and Authorization (formerly Certification and Accreditation)

System 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. OPM's process of certifying a system's security controls was formerly referred to as Certification and Accreditation (C&A), and is now referred to as Security Assessment and Authorization (Authorization).

Our FY 2008 and FY 2009 FISMA audit reports stated that weaknesses in OPM's C&A process were a significant deficiency in the internal control structure of the agency's IT security program. The weaknesses cited related to inadequate management of the process and incomplete, inconsistent, and poor quality C&A products. In FY 2010, these longstanding conditions continued to degrade, and as a result, they were reported as a material weakness in OPM's IT security program.

We reported that there were, in our opinion, three root causes of OPM's C&A issues: insufficient staffing in the IT Security and Privacy Group, a lack of policy and procedures, and the decentralized DSO model in place at OPM.

In FY 2011, the OCIO improved the policy deficiencies by publishing updated procedures and templates designed to improve the overall Authorization process and dedicating resources to facilitating Authorizations. We observed an improvement in the Authorization packages completed under this new process, and believe that this improvement warrants reducing the material weakness related to C&As to a significant

deficiency. Although no longer a material weakness, the Authorization process continues to be hindered by limited OCIO staffing resources and the decentralized DSO model (see section I, above).

The sections below provide a detailed evaluation of OPM's Authorization process.

a) Security Assessment and Authorization policy

In January 2011, the OCIO published a Security Assessment and Authorization Guide and several other procedures and templates that provide guidance to program offices certifying the security controls of each system. The OCIO has created and published guidance for completing the following elements of an Authorization:

- Information System Security Plan;
- FIPS 199 Security Categorization;
- Security Assessment Plan;
- Contingency Plan;
- Risk Assessment;
- System Registration;
- E-Authentication Assessment;
- System Security Plan; and,
- Interconnection Security Agreement.

We believe that the Security Assessment and Authorization Guide provides adequate guidance for certifying the security controls of information systems.

b) Quality and consistency of Authorization packages

The OIG reviewed the full Authorization packages of five systems that were subject to an Authorization after the OCIO issued the updated Security Assessment and Authorization Guide. The quality of all five packages appeared to be an improvement over security certifications completed under the former C&A process. However, as noted with C&A packages completed in the last several years, we continued to observe a wide range in quality between Authorization packages completed by various program offices (the specific problems and inconsistencies were provided to the OCIO but will not be detailed in this report).

The development of an Authorization package is the responsibility of the OPM program office that owns the system. Each program office assigns a DSO to manage the security of its systems. The decentralized nature of the DSO community at OPM means that individuals with varying skill sets are tasked with Authorization related responsibilities often as a collateral duty in addition to their normal job function. The existence of Authorization policies and procedures cannot be fully leveraged unless the individuals implementing them are consistently trained and dedicated to this function.

Recommendation 3

We recommend that the OCIO work with program offices to correct the specific errors that the OIG identified in the Authorization packages reviewed in FY 2011.

OCIO Response:

"The CIO Concurs with this recommendation and will take corrective action."

c) OCIO Management of the Authorization process

The OCIO is responsible for assisting program offices in the development of Authorization packages for their systems. OPM's Security Assessment and Authorization Guide also mandates OCIO involvement in all stages of the Authorization process for quality and completeness before recommending the system for authorization. In FY 2011, two full time resources were hired to review Authorization packages along with other IT security responsibilities. The most notable improvement made to the Authorization process was the implementation of three "decision points" at various steps of the Authorization process. At each decision point, representatives from the OCIO must review the work that has been completed and formally approve continuation of the Authorization process.

While we recognize the progress the OCIO has made in managing the Authorization process, we believe that there is still room for improvement. With additional resources dedicated to the review of Authorization packages, the inconsistencies referenced above could have been detected before the Authorization process was complete.

Recommendation 4 (*Rolled-Forward from 2010)*

We recommend that the OCIO assign additional resources to facilitate the Authorization process to ensure the consistency and quality of Authorization packages developed by OPM program offices.

OCIO Response:

"The CIO concurs with this recommendation and believes that additional security resources could improve the security authorization process. However, funding is not allocated in the CIO budget to hire additional resources."

III. Risk Management

NIST SP 800-37 Revision 1 "Guide for Applying the Risk Management Framework to Federal Information Systems" provides federal agencies with a framework for implementing an agency-wide risk management methodology. The Guide suggests that risk be assessed in relation to the agency's goals and mission from a three tiered approach: Tier 1: Organization (Governance); Tier 2: Mission/Business Process (Information and Information Flows); and Tier 3: Information System (Environment of Operation). NIST SP 800-39 "Managing Information Security Risk – Organization,

Mission, and Information System View" provides additional details of this three-tiered approach.

a) Agency-wide risk management

NIST SP 800-39 states that agencies should establish and implement "Governance structures [that] provide oversight for the risk management activities conducted by organizations and include:

(i) the establishment and implementation of a risk executive (function);
(ii) the establishment of the organization's risk management strategy including the determination of risk tolerance; and
(iii) the development and execution of organization-wide investment strategies for information resources and information security."

OPM's decentralized approach to IT security increases the need for an agency-wide risk management methodology, as the agency's mission is supported by multiple information systems owned by various program offices. Although the OCIO has made improvements in assessing risk at the individual system level (see Security Assessment and Authorization section II, above), the OCIO does not currently have a formal methodology for managing risk at an organization-wide level.

In FY 2011, the OCIO organized a Risk Executive Function comprised of several IT security professionals. However, the 12 primary functions of the Risk Executive Function as explained in NIST SP 800-39 section 2.3.2, Risk Executive Function, are not all fully implemented.

Recommendation 5

We recommend that the OCIO develop policies and procedures related to managing risk from an agency-wide perspective.

OCIO Response:

"The CIO does not concur with this recommendation and believes that adequate policies and procedures are in place to manage risk from an agency-wide perspective as documented in sections 3.1.9 and 3.1.7 of the IT Security Handbook dated March 31, 2011."

OIG Reply:

The majority of the text in sections 3.1.7 and 3.1.9 of the IT Security Handbook is copied verbatim from NIST SP 800-53 Rev 3, and the handbook contains no guidance on agency-wide risk management specific to OPM.

Among the limited original text in these sections of the Handbook is the statement "OPM shall: Develop a comprehensive strategy to manage risk to OPM operations and assets. . . ." However, the OIG has received no evidence that OPM has developed a risk management strategy or the associated policies and procedures.

We continue to recommend that the OCIO develop policies and procedures related to managing risk from an agency-wide perspective.

Recommendation 6

We recommend that the OCIO continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive (Function).

OCIO Response:

"The CIO concurs with this recommendation and will take the necessary corrective action."

b) System specific risk management

NIST SP 800-37 Revision 1 outlines a risk management framework (RMF) that contains six primary steps, including (i) the *categorization* of information and information systems; (ii) the *selection* of security controls; (iii) the *implementation* of security controls; (iv) the *assessment* of security control effectiveness; (v) the *authorization* of the information system; and, (vi) the ongoing *monitoring* of security controls and the security state of the information system."

The OCIO has implemented the six step RMF into its system-specific risk management activities through the new Authorization process; see section II above for a description of OPM's Authorization methodology.

c) System security control testing

Although a full Authorization package is required for each system every three years, the security controls of that system must be tested on an annual basis. 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.

We reviewed documentation resulting from the security controls tests for each system in OPM's inventory. Our evaluation indicated that the IT security controls had been adequately tested for only 36 of OPM's 48 systems during FY 2011. 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.

OPM's decentralized approach to IT security places responsibility on the various program offices for testing the security controls of their systems. The OCIO's lack of authority over these program offices has contributed to the inadequate security control testing of the agency's information systems.

Recommendation 7 (*Rolled-Forward from 2008)*

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

OCIO Response:

"The CIO concurs with this recommendation and offers the following clarifying remarks in order to present a more current interpretation. In FY2011 security controls testing was completed for 41 of 48 eligible systems resulting in an 85% compliance rate. In FY2012, we will continue to work with program offices to ensure that security controls are tested for all eligible systems."

OIG Reply:

We disagree that 41 out of 48 eligible systems were subject to an adequate security controls test in FY 2011. The OCIO's count of 41 includes 4 systems that were granted an extension and one system that does not have adequate support that a test was conducted. We do not believe that any extensions should be granted; every system must be subjected to a security controls test every fiscal year.

IV. Configuration Management

The sections below detail 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's OCIO has implemented an agency-wide Information Security and Privacy Policy Handbook that defines the requirements necessary to meet the fundamental security and privacy objectives of confidentiality, integrity, and availability. The handbook includes a section devoted to configuration management. The OCIO also maintains a comprehensive configuration management policy that outlines the process and procedures for maintaining a securely configured network environment.

b) Standard baseline configurations

The OCIO maintains standard baseline configurations and/or build sheets for all operating platforms used by OPM to support major applications, including:

- Windows Server 2000;
- Windows Server 2003;
- Windows Server 2008;
- Linux;
- Oracle; and,
- Microsoft SQL.

The OCIO uses vulnerability scanning tools to routinely scan servers to ensure compliance with configuration guides and baselines for these operating platforms. Nothing came to our attention during this review to indicate that there are weaknesses in OPM's baseline configuration controls.

c) Vulnerability Scanning

The OCIO performs scans of all production servers using automated vulnerability scanning tools. Although vulnerability scanning occurs on a continuous basis, the OCIO does not have a formal process to manage weaknesses identified in the scanning reports.

Daily security advisory reports are sent to OCIO managers and a weekly roll-up report is generated to summarize weekly vulnerability scanning activity. Although we verified that these reports are routinely distributed, we were unable to determine what, if any, activity is done to review and analyze the vulnerabilities identified. At a minimum we recommend implementing a vulnerability tracking methodology that includes steps to:

- identify false positives in vulnerability scanning reports;
- identify and document vulnerabilities that the agency "accepts" and does not intend to fix; and,
- formally document and track the remaining vulnerabilities until they are remediated.

Recommendation 8

We recommend that the OCIO implement a process for tracking the status of weaknesses identified through vulnerability scanning.

OCIO Response:

"The CIO concurs with this recommendation and will implement the necessary corrective action."

Recommendation 9

We recommend that the OCIO document "accepted" weaknesses identified in vulnerability scans.

OCIO Response:

"The CIO concurs with this recommendation and will implement the necessary corrective action."

d) Management of hardware inventory

The OCIO currently maintains a centralized agency-wide hardware inventory. The OCIO uses several automated tools to scan the network environment to track and

verify hardware inventories. They also maintain an inventory of all OPM owned user workstations. Each workstation is cataloged before being placed into service.

e) Federal Desktop Core/United States Government Computer Baseline Configuration

OPM has developed a Windows XP standard image that is generally compliant with Federal Desktop Core Configuration (FDCC) standards and has documented nine deviations between this image and FDCC requirements. OPM has also developed and tested a United States Government Baseline Configuration compliant image for all Windows 7 workstations. These images have been installed on all OPM workstations with this operating system.

V. Incident Response and Reporting

OPM's "Incident Response and Reporting Guide" 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 Guide requires any user of the agency's IT resources to immediately notify OPM's Situation Room when IT security incidents occur. The agency also currently uses two distinct intrusion detection systems to monitor network traffic for abnormalities. In addition, OPM reiterates the information provided in the Incident Response and Reporting Guide in the annual IT security and privacy awareness training.

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.

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. OPM notifies the OIG's Office of Investigations of security incidents with a monthly report outlining all incidents where sensitive data was lost.

VI. Security Training

All OPM employees are required to take IT security awareness training on an annual basis. In addition, employees with IT security responsibility are required to take additional specialized training.

a) IT security awareness training

The OCIO provides annual IT security and privacy awareness training to all OPM employees 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 code, 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 2011.

b) Specialized IT security training

Agency employees with significant information security responsibilities are required to take specialized security training in addition to the annual awareness training.

The OCIO has developed a table outlining the security training requirements for specific job roles by groups. The OCIO uses a spreadsheet to track the security training taken by employees that have been identified as having security responsibility. Of those identified, only 75 percent have completed at least one hour of specialized security training in FY 2011.

Recommendation 10 (*Rolled-Forward from 2010)*

We continue to recommend that the OCIO ensure that all employees with significant information security responsibility take meaningful and appropriate specialized security training on an annual basis.

OCIO Response:

"The CIO concurs with this recommendation and offers the following clarifying remarks. In FY2011, we redesigned the OPM specialized security training program as part of our risk management strategy and to improve accuracy. We achieved a success rate of 75% and for the first time identified and required Executives and senior staff serving as Authorizing Officials and System Owners to complete the required training."

VII. Plan of Action and Milestones

A POA&M is a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for IT security weaknesses. In FY 2010, the OCIO developed a POA&M Guide that provides a template and instructions for system owners to use in managing known IT security weaknesses. The sections below detail OPM's effectiveness in using POA&Ms to track the agency's security weaknesses.

a) POA&Ms incorporate all known IT security weaknesses

In October 2010, we issued the FY 2010 FISMA audit report with 41 audit recommendations. We verified that all 41 of the recommendations were appropriately incorporated into the OCIO POA&M.

We reviewed 14 system POA&Ms submitted to the OCIO in FY 2011 to determine if all known IT security weaknesses identified in the annual security controls tests were incorporated into the quarterly POA&Ms. Nothing came to our attention to indicate that program offices were not incorporating all known IT security weaknesses into system POA&Ms.

b) 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 up-to-date POA&Ms were submitted to the OCIO on a quarterly basis for all 48 OPM systems.

c) Remediation plans for correcting security weaknesses

When a POA&M item is remediated, OPM program offices are required to submit a work completion plan (WCP) along with evidence that the deficiency was corrected to the OCIO for review. We reviewed WCPs for eight systems and found that the program offices provided sufficient evidence that the weaknesses were corrected. The 8 systems were selected from the 48 OPM systems and were judgmentally chosen by OIG auditors. The results of the sample test were not projected to the entire population.

d) Compliance with estimated dates for remediation

The POA&Ms for 10 OPM systems contain security weaknesses with remediation activities over 120 days overdue. In the 3rd quarter of 2011, OPM systems had a total of 36 POA&M items over 120 days overdue, an improvement from the 58 overdue items during the same time period in FY 2010.

Program offices are responsible for dedicating adequate resources to addressing POA&M weaknesses and meeting target objectives. In FY 2011, the OCIO provided

improved guidance to ensure that program offices assign reasonable POA&M due dates and stay on track to meet those dates.

e) 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. The POA&Ms for all systems in OPM's inventory adequately prioritized security weaknesses.

VIII. Remote Access Management

The OIG evaluated OPM's remote access and telecommuting policies and procedures and its progress in implementing the requirements of NIST SP 800-46 Revision 1, "Guide to Enterprise Telework and Remote Access Security." In FY 2011, the OCIO developed an updated remote access policy. The new policy contains all of the critical elements required by the NIST guide.

We also evaluated OPM's progress in enforcing two-factor authentication for remote users.

a) Authentication requirements

OPM utilizes a Virtual Private Network (VPN) client to provide remote users with secure access to the agency's network environment. The VPN requires users to uniquely identify and authenticate themselves, and the OCIO maintains logs of individuals who remotely access the network. The logs are reviewed on a monthly basis for unusual activity or trends.

In FY 2009, OPM required two-factor authentication for remote access in the form of RSA token devices in combination with a password. However, the agency stopped enforcing two-factor authentication in FY 2010 and users were able to authenticate with only a password. In FY 2011, the OCIO implemented the capability of using Personal Identity Verification (PIV) cards along with a password for two-factor authentication. However, there is still a subset of users who can access the network remotely using only a static password.

Recommendation 11 (*Rolled-Forward from 2010)*

We recommend that CIO enforce two-factor authentication with PIV cards for all remote access to its network environment.

OCIO Response:

"The CIO concurs with this recommendation and offers the following clarification remarks. The OPM network is now configured for two factor authentication with PIV cards and most remote users are using PIV cards for authentication. In

FY2012, we will continue to work on having the remaining users who are not using PIV cards for authentication to comply with this requirement."

IX. Identity and Access Management

The sections below detail OPM's account and identity management program.

a) Account management

OPM maintains policies related to management of user accounts for its local area network (LAN) and its mainframe environments. Both policies contain procedures for creating user accounts with the appropriate level of access as well as procedures for removing access for terminated employees.

The OIG compared a list of recently terminated OPM employees to a list of active LAN and mainframe users. We found that 17 employees maintained LAN access after their termination date, and 7 users had multiple accounts. We found no issues of mainframe users maintaining access after their termination.

OPM's human resources department is responsible for creating and distributing a weekly list of terminated employees. This list is e-mailed directly to the mainframe team. However, nobody from the LAN team is copied on the distribution. We were not informed of any audits/reviews conducted on user accounts by the LAN team. However, any audit activity is not sufficient as evidenced by the account violations detected during our review.

Failure to promptly remove LAN access for terminated employees increases the risk that individuals could gain unauthorized access to sensitive data stored on OPM's network environment.

Recommendation 12

We recommend that all LAN accounts assigned to terminated employees be disabled.

OCIO Response:

"The CIO concurs with this recommendation and offers the following clarification. Currently, LAN accounts assigned to terminated employees are disabled once the information is provided to the Help Desk. However, there are occasions when the help desk does not always receive timely notification of terminated employees."

Recommendation 13

We recommend that all unnecessary duplicate user accounts be disabled.

OCIO Response:

"The CIO concurs with this recommendation and will take the necessary corrective action."

Recommendation 14

We recommend that the human resources employee termination list be distributed to all information system owners.

OCIO Response:

"There is concurrence with this recommendation. [OPM Human Resources (OPMHR)] has no objection in principle to supplying the separation list that is currently distributed to some system owners to all system owners as identified by the CIO; however, a quick review of the list shows some significant ownership issues.

1. ***OPMHR will review the ownership list in its' entirety and reserves the right to make adjustments either based on its' personal knowledge of the system and its' ownership or after consultation with the listed owner.***
2. ***There are multiple versions of the separation report. Due to the additional number of recipients, OPMHR will work with the system owners to develop a generic report to minimize the workload impact."***

OIG Reply:

We acknowledge the fact that OPMHR agrees to provide the termination list. In order to fully address this recommendation, the OCIO must provide OPMHR with a list of appropriate recipients.

Recommendation 15

We recommend that the OCIO implement a process to routinely audit all active user accounts to search for terminated employees or duplicate accounts.

OCIO Response:

"The CIO concurs with this recommendation and will take the necessary corrective action."

b) Unauthenticated network devices

The OCIO maintains an inventory of user workstations and servers connected to the OPM network environment. In FY 2010, the OCIO tested an automated tool that would scan the network for rogue devices not associated with authenticated users. The OCIO stated that "An automated process to detect unauthenticated network devices has been procured and is expected to be in place and operational in the third quarter FY 2011." However, this control has not yet been implemented.

Recommendation 16 (*Rolled-Forward from 2010)*

We recommend that the OCIO implement an automated process to detect unauthenticated network devices.

OCIO Response:

"The CIO concurs with this recommendation and will take the necessary corrective action."

X. Continuous Monitoring Management

The following sections detail OPM's controls related to continuous monitoring of the security state of its information systems.

a) Continuous monitoring policy and procedures

OPM's Information Security and Privacy Policy Handbook states that the security controls of all systems must be continuously monitored and assessed annually to ensure continued effectiveness.

In FY 2011, the OCIO developed a Continuous Monitoring Working Group tasked with implementing a continuous monitoring program at the agency. The working group has developed a Concept of Operations (CONOPS) document that outlines the framework for the planned continuous monitoring program.

Although the creation of the working group and the CONOPS indicates that the OCIO has taken steps toward implementing a continuous monitoring program at OPM, this project remains a work in progress.

Recommendation 17 (*Rolled-Forward from 2010)*

We recommend OPM develop a Continuous Monitoring Policy that outlines a strategy for identifying information security controls that need continuous monitoring as well as procedures for conducting the tests.

OCIO Response:

"The CIO concurs with this recommendation and work is already underway to develop an OPM Continuous Monitoring program which will include policies and procedures."

b) Common security controls

In FY 2011, the OCIO developed a catalog of information security controls that are shared ("common") with all of the agency's applications. Common security controls do not need to be tested for individual applications "inheriting" these controls, as they have already been certified at an agency-wide level. The existence of the common controls catalog saves time and resources by eliminating the need for these controls to be tested multiple times by each application that inherits them.

The current common controls catalog indicates that approximately 25% of the security controls outlined in NIST SP 800-53 Revision 3, "Recommended Security

Controls for Federal Information Systems," are common to all agency applications. However, the vast majority of these common controls are related to policy or program management. The current version of the catalog is incomplete, as it does not account for the large number of technical controls that are common to applications residing on one of OPM's several general support systems. The OCIO indicated that it intends to update the catalog with additional common controls.

Recommendation 18 (*Rolled-Forward from 2010)*

We recommend that OPM create a comprehensive list of common security controls and distribute this information to OPM program offices responsible for testing individual applications.

OCIO Response:

"The CIO does not concur with this recommendation and offers the following clarifying remarks. In FY2011, over 50 common controls were identified by the CISO and independently tested by the Bureau of Public Debt [BPD]. These common security controls were published August 2011 on THEO and is available to all OPM program offices. In FY2012, we will identify and independently test additional security controls that are candidates for common control status."

OIG Reply:

The majority of controls contained within OPM's catalog are related to policies and procedures. We continue to assert that the current version of the catalog is incomplete, as it does not account for the large number of technical controls that are common to applications residing on one of OPM's several general support systems. The current OPM common controls catalog adds minimal value to the main objective of a comprehensive catalog: saving time and resources by eliminating the need for these controls to be tested multiple times by each application that inherits them.

We continue to recommend that OPM create a comprehensive list of common security controls and distribute this information to OPM program offices responsible for testing individual applications. We will consider this recommendation to be implemented when the common controls catalog contains the technical controls provided by OPM general support systems.

XI. Contingency Planning

OPM's Information Security Privacy and Policy Handbook requires a contingency plan to be in place for each federal information system. We verified that contingency plans exist for all 48 production systems on OPM's master system inventory.

In prior OIG FISMA audits, we noted that the quality and consistency of contingency plans varied greatly between OPM's various systems. As a result, the OCIO developed a contingency plan template that all system owners are now required to use. The new template closely follows the guidance of NIST SP 800-34, Contingency Planning Guide

for Information Technology Systems. Use of the new template is required for all systems that start the security authorization process after January 2011. As of August 2011, only six systems have conducted an authorization using the new guidance. The quality and consistency of the contingency plans appears to be improving with the use of the new template.

a) Testing contingency plans of individual OPM systems

OPM's Information Security Privacy and Policy Handbook requires that "The contingency plan for the information system is tested and/or exercised at least annually using OPM defined and information system specific tests and exercises. . . ." We received evidence that contingency plans were tested for only 40 of 48 systems in FY 2011.

Of the contingency plan tests we did receive, we continue to notice inconsistency in the quality of the documentation produced for various OPM systems. One of the main areas of inconsistency relates to the contingency plan test after action report. NIST SP 800-34 states that following a contingency plan test, "results and lessons learned should be documented and reviewed by test participants and other personnel as appropriate. Information collected during the test and post-test reviews that improve plan effectiveness should be incorporated into the contingency plan." Several after action reports we reviewed did not include summarized results or lessons learned. Without a thoroughly documented after action report, system owners will not know how to improve the contingency plan in order to be better prepared for a disruptive event.

These inconsistencies were the result of the program offices not having adequate guidance for conducting contingency plan tests at the time the tests were completed. The OCIO recently issued detailed guidance to program offices on how to conduct a contingency plan test and create an after action report. As part of the FY 2012 FISMA audit, we will test the impact that this new guidance has on the quality of system level contingency plan tests.

Recommendation 19 (*Rolled-Forward from 2008)*

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 8 systems that were not subject to adequate testing in FY 2011.

OCIO Response:

"The CIO concurs with this recommendation."

b) Agency-wide coordination of contingency plan testing

Many OPM systems reside on one of the agency's general support systems. While the contingency plans for these general support systems are tested on an individual basis, there is no coordinated contingency plan or disaster recovery test. A

coordinated test is critical because there are several applications that have elements or modules spread across multiple general support systems. Without some form of centralized approach to contingency plan testing there is a risk that OPM systems will not be successfully recovered in the event of a disaster.

The agency has also not completed an agency-wide business impact analysis (BIA). OPM's Security Assessment and Authorization Guide states that "In order to properly develop a [Contingency Plan], a Business Impact Analysis must first be conducted. The BIA provides the necessary risk determinations to develop the system contingency plan." OPM is in the process of creating an agency-wide BIA, but this was not completed in FY 2011. Without a BIA, the agency cannot adequately prioritize the recovery of agency systems to facilitate a successful disaster recovery process.

Recommendation 20

We recommend that the OCIO conduct an agency-wide Business Impact Analysis.

OCIO Response:

"The CIO concurs with this recommendation and will take the necessary corrective action."

Recommendation 21

We recommend that the OCIO implement and document a centralized (agency-wide) approach to contingency plan testing.

OCIO Response:

"The CIO concurs with this recommendation but seeks clarifying information from the OIG on this recommendation."

OIG Reply:

We will provide the OCIO additional information on this recommendation, but the details will not be contained within this audit report.

XII. Contractor Systems

OPM's master system inventory indicates that 16 of the agency's 48 major applications are operated by a contractor.

We evaluated the methods that various program offices use to maintain oversight of their systems run by contractors. In response to a FY 2010 FISMA audit recommendation regarding oversight of contractor-operated systems, the OCIO created a Site Survey Assessment form that program offices had to complete for all contractor-operated systems. The survey asked the program office to comment on the security controls in place at the contractor facilities. The survey was a positive step in providing oversight

over contractor-operated systems. Although the program offices appeared to provide an adequate level of oversight to contractor-operated systems, the techniques and quality of this oversight was inconsistent between program offices. This inconsistency is the result of OPM not having an agency-wide policy related to oversight of contractor systems.

Recommendation 22

We recommend that, in addition to the Site Survey Assessment Form, OPM develop a policy providing guidance on adequate oversight of contractor-operated systems.

OCIO Response:

"The CIO partially concurs with this recommendation and believes that existing security policy also applies to contractor systems as documented under the Federal Information Security Management Act of 2002. However, the CIO believes that additional policy clarifications would be beneficial to improving security for OPM contractor systems and will update policy accordingly."

OIG Reply:

Although OPM's IT Security Handbook may apply to contractors, we determined that the techniques and quality of oversight provided to contractor systems was inconsistent between program offices. This inconsistency is the result of OPM not having an agency-wide policy providing program offices guidance on overseeing the activities of contractors operating OPM systems. We continue to recommend that the OCIO develop policies to address oversight of contractor systems.

XIII. Security Capital Planning

NIST SP 800-53 section SA-2, Allocation of Resources, states that an organization needs to determine, document, and allocate the resources required to protect information systems as part of its capital planning and investment control process.

OPM's Information Security and Privacy Policy Handbook contains policies and procedures to ensure that information security is addressed in the capital planning and investment process. The OCIO uses Exhibit 53B to record information security resources allocation and submits this information annually to OMB.

Nothing came to our attention to indicate that OPM does not maintain an adequate capital planning and investment program for information security.

XIV. Follow-up of Prior OIG Audit Recommendations

All audit recommendations issued prior to 2010 were rolled forward into one of the recommendations in the FY 2010 OIG FISMA audit report (Report 4A-CI-00-10-019). FY 2010 recommendations that were not remediated by the end of FY 2011 are rolled forward with a new recommendation number in this FY 2011 OIG FISMA audit report.

The prior sections of this report evaluate the current status of many 2010 recommendations. However, there are several recommendations that have not yet been addressed because the related topics were not part of the FY 2011 FISMA reporting instructions. These remaining recommendations are addressed in the sections below.

Note - Audit recommendations issued prior to FY 2010 reference OPM's Center for Information Services (CIS) as the program office responsible for the agency's IT security program. After an organizational realignment, this group is now referred to as the Office of the Chief Information Officer (OCIO).

Follow-up on recommendations issued in OIG Audit Report 4A-CI-00-10-019, "Federal Information Security Management Act Audit – FY 2010"

a) 4A-CI-00-10-019 Recommendation 3
We recommend that the OCIO develop and implement an active strategy to maintain up-to-date information regarding OPM's master system inventory.

FY 2011 Status
The OCIO conducted an inventory survey of OPM program offices in FY 2010. However, one program office has not yet responded to the survey. This recommendation remains open and is rolled forward in FY 2011.

Recommendation 23 (*Rolled-Forward from 2010*)
We recommend that the OCIO develop and implement an active strategy to maintain up-to-date information regarding OPM's master system inventory.

OCIO Response:

"The CIO does not concur with this recommendation and believes that existing methods for maintaining the OPM master systems inventory are adequate. These methods consist of requiring DSOs to provide monthly system inventory updates to the CISO and the CISO conducts an annual survey to identify systems at contractor facilities, other Federal agencies or internal to OPM."

OIG Reply:

One OPM program office has not responded to the OCIO's survey regarding information system inventory. Without full participation from OPM program offices, the OCIO's approach of identifying information systems via surveys is not adequate.

b) 4A-CI-00-10-019 Recommendation 33 *(Roll-forward from OIG Report 4A-CI-00-09-031 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.

FY 2011 Status
The OCIO conducted an inventory survey of OPM program offices in FY 2010. However, one program office has not yet responded to the survey. This recommendation remains open and is rolled forward in FY 2011.

Recommendation 24 (*Rolled-Forward from 2009)*
We recommend that CIS conduct a survey of OPM program offices 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.

OCIO Response:

"The CIO concurs with this recommendation and offers the following clarifying remarks. In FY2011, we conducted a survey of OPM program offices to identify systems that should be added to the system inventory. In FY2012, we plan to conduct another survey and identified systems will be added to the system inventory."

OIG Reply:

If the OCIO does not receive full participation by OPM program offices to the 2012 survey, we recommend that they develop a new methodology for identifying information systems owned by the agency.

c) 4A-CI-00-10-019 Recommendation 35 (*Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 4*)
We recommend that CIS conduct a survey to determine how many systems owned by another agency are used by OPM.

FY 2011 Status
The OCIO conducted an inventory survey of OPM program offices in FY 2010. We discovered that one program office did not respond to the survey. This recommendation remains open and is rolled forward in FY 2011.

Recommendation 25 (*Rolled-Forward from 2009)*
We recommend that CIS conduct a survey to determine how many systems owned by another agency are used by OPM.

OCIO Response:

"The CIO concurs with this recommendation and offers the following clarifying remarks. In FY2011, we conducted a survey of OPM program offices to identify systems owned by another agency and used by OPM. In FY2012, we plan to conduct another survey and identified systems will be added to the system inventory."

OIG Reply:

If the OCIO does not receive full participation by OPM program offices to the 2012 survey, we recommend that they develop a new methodology for identifying information systems owned by the agency.

d) 4A-CI-00-10-019 Recommendation 37 (*Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 20*)
We recommend that a new PIA be conducted for the appropriate systems based on the updated PIA Guide.

FY 2011 Status
All agency systems have not completed a PIA using the new format. This recommendation remains open and is rolled forward in FY 2011.

Recommendation 26 (*Rolled-Forward from 2009)*
We recommend that a new PIA be conducted for the appropriate systems based on the updated PIA Guide.

OCIO Response:

"The CIO concurs with this recommendation and offers the following remarks. All PIAs with the exception of four were updated to reflect the new PIA Guide. We will take corrective action to ensure that the remaining four are updated."

e) 4A-CI-00-10-019 Recommendation 38 *(Roll-forward from OIG Report 4A-CI-00-09-031 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 the OCIO.

FY 2011 Status
All agency systems have not completed a PIA using the new format and therefore cannot adequately reevaluate their current holdings of PII. This recommendation remains open and is rolled forward in FY 2011.

Recommendation 27 (*Rolled-Forward from 2009)*
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 the OCIO.

OCIO Response:

"The CIO does not concur with this recommendation and believes that all PIAs were reviewed by system owners in FY2011."

OIG Reply:

Four systems do not have current PIAs; therefore all PIAs were not reviewed by system owners in FY 2011.

f) 4A-CI-00-10-019 Recommendation 39 (*Roll-Forward from OIG Reports 4A-CI-00-09-031 Recommendation 22 and 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.

FY 2011 Status
The OCIO has an ongoing plan to reduce and eventually eliminate the unnecessary use of SSNs. However, resource limitations prevented them from completing this task in FY 2011**.** This recommendation remains open and is rolled forward in FY 2011.

Recommendation 28 (*Rolled-Forward from 2008)*
We recommend that OPM continue its efforts to eliminate the unnecessary use of SSNs in accordance with OMB Memorandum M-07-16.

OCIO Response:

"The CIO concurs with this recommendation and offers the following clarifying remarks. OPM currently does not have the funding to effectively pursue the elimination of unnecessary use of SSN's as stated in OMB memorandum M-07-16. Efforts are made when the unnecessary use of SSN is discovered in PTA and PIA documentation and efforts are explored with the program office for alternatives. OPM does comply with the requirement to meet regularly with other federal agencies on this effort."

g) 4A-CI-00-10-019 Recommendation 40 (*Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 27*)
We recommend OPM incorporate Federal Acquisition Regulation 2007-004 language in all contracts related to common security settings.

FY 2011 Status
The OCIO is in the process of incorporating Federal Acquisition Regulation 2007-004 language in all contracts related to common security settings. However, they did not finish this process in FY 2011. This recommendation remains open and is rolled forward in FY 2011.

Recommendation 29 (*Rolled-Forward from 2009)*
We recommend OPM incorporate Federal Acquisition Regulation 2007-004 language in all contracts related to common security settings.

OCIO Response:

"The CIO concurs with this recommendation and will take the necessary corrective action."

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], Senior Team Leader
- [redacted] IT Auditor
- [redacted], IT Auditor
- [redacted], IT Auditor

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Information Officer

MEMORANDUM FOR [redacted]
CHIEF
INFORMATION SYSTEMS AUDIT GROUP

FROM: MATTHEW E. PERRY
CHIEF INFORMATION OFFICER
Oct 21, 2011

Subject: Response to the Federal Information Security Management Act Audit – FY2011, Report NO. 4A-CI-00-11-009

Thank you for the opportunity to comment on the subject report. The results provided in the draft report consist of a number of recommendations. The recommendations are valuable to our program improvement efforts and most of them are generally consistent with our plan. We plan to continue making improvements in our security risk management strategy and the OPM IT security program.

OIG Recommendations:

Recommendation 1
We recommend that the OCIO develop policies to address oversight of contractor systems, IV&V, and continuous monitoring of high risk security controls.

The CIO partially concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The policies in the IT Security Handbook dated March 31, 2011 apply to all OPM systems including those at contractor facilities and therefore a new policy for oversight of contractor systems is not necessary. The CIO believes that new policies for IV&V and continuous monitoring of high risk security controls should be developed and would be beneficial to the OPM security program.

Recommendation 2 (*Rolled-Forward from 2010*)
We recommend that OPM implement a centralized information security governance structure where all information security practitioners, including designated security officers, report to the SAISO. Adequate resources should be assigned to the OCIO to create this structure. Existing designated security officers who report to their program offices should return to their program office duties. The new staff that reports to the SAISO should consist of experienced information security professionals.

The CIO concurs with this recommendation and offers the following remarks. The CIO's budget does not contain funding to replace the Designated Security Officers with information security

professionals. One possible suggestion is to require OPM program offices to provide funding for the CIO to hire information security professionals.

Recommendation 3
We recommend that the OCIO work with program offices to correct the specific errors that the OIG identified in the Authorization packages reviewed in FY 2011.

The CIO Concurs with this recommendation and will take corrective action.

Recommendation 4 *(Rolled-Forward from 2010)*
We recommend that the OCIO assign additional resources to facilitate the Authorization process to ensure the consistency and quality of Authorization packages developed by OPM program offices.

The CIO concurs with this recommendation and believes that additional security resources could improve the security authorization process. However, funding is not allocated in the CIO budget to hire additional resources.

Recommendation 5
We recommend that the OCIO develop policies and procedures related to managing risk from an agency-wide perspective.

The CIO does not concur with this recommendation and believes that adequate policies and procedures are in place to manage risk from an agency-wide perspective as documented in sections 3.1.9 and 3.1.7 of the IT Security Handbook dated March 31, 2011.

Recommendation 6
We recommend that the OCIO continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive (Function).

The CIO concurs with this recommendation and will take the necessary corrective action.

Recommendation 7 *(Rolled-Forward from 2008)*
We recommend that OPM ensure that an annual test of security controls has been completed for all systems.

The CIO concurs with this recommendation and offers the following clarifying remarks in order to present a more current interpretation. In FY2011 security controls testing was completed for 41 of 48 eligible systems resulting in an 85% compliance rate. In FY2012, we will continue to work with program offices to ensure that security controls are tested for all eligible systems.

Recommendation 8
We recommend that OCIO implement a process for tracking the status of weaknesses identified through vulnerability scanning.

The CIO concurs with this recommendation and will implement the necessary corrective action.

Recommendation 9
We recommend that OCIO document "accepted" weaknesses identified in vulnerability scans.

The CIO concurs with this recommendation and will implement the necessary corrective action.

Recommendation 10 *(Rolled-Forward from 2010)*
We continue to recommend that the OCIO ensure that all employees with significant information security responsibility take meaningful and appropriate specialized security training on an annual basis.

The CIO concurs with this recommendation and offers the following clarifying remarks. In FY2011, we redesigned the OPM specialized security training program as part of our risk management strategy and to improve accuracy. We achieved a success rate of 75% and for the first time identified and required Executives and senior staff serving as Authorizing Officials and System Owners to complete the required training.

Recommendation 11 *(Rolled-Forward from 2010)*
We recommend that CIO enforce two-factor authentication with PIV cards for all remote access to its network environment.

The CIO concurs with this recommendation and offers the following clarification remarks. The OPM network is now configured for two factor authentication with PIV cards and most remote users are using PIV cards for authentication. In FY2012, we will continue to work on having the remaining users who are not using PIV cards for authentication to comply with this requirement.

Recommendation 12
We recommend that all LAN accounts assigned to terminated employees be disabled.

The CIO concurs with this recommendation and offers the following clarification. Currently, LAN accounts assigned to terminated employees are disabled once the information is provided to the Help Desk. However, there are occasions when the help desk does not always receive timely notification of terminated employees.

Recommendation 13
We recommend that all unnecessary duplicate user accounts be disabled.

The CIO concurs with this recommendation and will take the necessary corrective action.

Recommendation 14
We recommend that the human resources employee termination list be distributed to all information system owners.

There is concurrence with this recommendation. OPMHR has no objection in principle to supplying the separation list that is currently distributed to some system owners to all system owners as identified by the CIO; however, a quick review of the list shows some significant ownership issues.

1. OPMHR will review the ownership list in its' entirety and reserves the right to make adjustments either based on its' personal knowledge of the system and its' ownership or after consultation with the listed owner.
2. There are multiple versions of the separation report. Due to the additional number of recipients, OPMHR will work with the system owners to develop a generic report to minimize the workload impact.

We wish to state that receipt of this report may not facilitate the earliest termination of network accounts for the following reasons:

1. HR relies on individual organizations to submit separation actions for their employees. We do not know when someone leaves the agency until we receive that notification.
2. In the case of employees who transfer to another agency, published government-wide guidance states that the employee cannot be removed from the rolls until positive evidence of the transfer from the gaining agency is received. In those cases we are at the mercy of the other agency to notify us. It is not unusual for it to take months to receive this notification.

Several years ago the agency's Exit Clearance Process was reviewed and revised based on this very issue. An agency-wide working group was pulled together to review the process and come up with a workable solution. The responsibility for clearing an employee from the building rested with the employee's supervisor and they were responsible for making sure that any equipment was returned as well as their employee ID was turned it. You might want to think about revisiting that process at this time.

Recommendation 15

We recommend that the OCIO implement a process to routinely audit all active user accounts to search for terminated employees or duplicate accounts.

The CIO concurs with this recommendation and will take the necessary corrective action.

Recommendation 16 *(Rolled-Forward from 2010)*

We recommend that the OCIO implement an automated process to detect unauthenticated network devices.

The CIO concurs with this recommendation and will take the necessary corrective action.

Recommendation 17 (*Rolled-Forward from 2010*)
We recommend OPM develop a Continuous Monitoring Policy that outlines a strategy for identifying information security controls that need continuous monitoring as well as procedures for conducting the tests.

The CIO concurs with this recommendation and work is already underway to develop an OPM Continuous Monitoring program which will include policies and procedures.

Recommendation 18 (*Rolled-Forward from 2010*)
We recommend OPM create a list of common security controls and distribute this information to OPM program offices responsible for testing individual applications.

The CIO does not concur with this recommendation and offers the following clarifying remarks. In FY2011, over 50 common controls were identified by the CISO and independently tested by the Bureau of Public Debt. These common security controls were published August 2011 on THEO and is available to all OPM program offices. In FY2012, we will identify and independently test additional security controls that are candidates for common control status.

Recommendation 19 (*Rolled-Forward from 2008*)
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 28 systems that were not subject to adequate testing in FY 2011.

The CIO concurs with this recommendation and offers the following clarifying remarks in order to present a more current interpretation. In FY2011 contingency plan testing was completed for 40 of 48 eligible systems resulting in an 83% compliance rate. In FY2012, we will continue to work with program offices to ensure that contingency plan testing is conducted for all eligible systems.

Recommendation 20
We recommend that the OCIO conduct an agency-wide Business Impact Analysis.

The CIO concurs with this recommendation and will take the necessary corrective action

Recommendation 21
We recommend that OCIO implement and document a centralized (agency-wide) approach to contingency plan testing.

The CIO concurs with this recommendation but seeks clarifying information from the OIG on this recommendation.

Recommendation 22
We recommend that, in addition to the Site Survey Assessment Form, OPM develop a policy providing guidance on adequate oversight of contractor-operated systems.

The CIO partially concurs with this recommendation and believes that existing security policy also applies to contractor systems as documented under the Federal Information Security Management Act of 2002. However, the CIO believes that additional policy clarifications would be beneficial to improving security for OPM contractor systems and will update policy accordingly.

Recommendation 23 *(Rolled-Forward from 2010)*
We recommend that the OCIO develop and implement an active strategy to maintain up-to-date information regarding OPM's master system inventory.

The CIO does not concur with this recommendation and believes that existing methods for maintaining the OPM master systems inventory are adequate. These methods consist of requiring DSOs to provide monthly system inventory updates to the CISO and the CISO conducts an annual survey to identify systems at contractor facilities, other Federal agencies or internal to OPM.

Recommendation 24 *(Rolled-Forward from 2009)*
We recommend that CIS conduct a survey of OPM program offices 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.

The CIO concurs with this recommendation and offers the following clarifying remarks. In FY2011, we conducted a survey of OPM program offices to identify systems that should be added to the system inventory. In FY2012, we plan to conduct another survey and identified systems will be added to the system inventory.

Recommendation 25 *(Rolled-Forward from 2009)*
We recommend that CIS conduct a survey to determine how many systems owned by another agency are used by OPM.

The CIO concurs with this recommendation and offers the following clarifying remarks. In FY2011, we conducted a survey of OPM program offices to identify systems owned by another agency and used by OPM. In FY2012, we plan to conduct another survey and identified systems will be added to the system inventory.

Recommendation 26 *(Rolled-Forward from 2009)*
We recommend that a new PIA be conducted for the appropriate systems based on the updated PIA Guide.
The CIO concurs with this recommendation and offers the following remarks. All PIAs with the exception of four were updated to reflect the new PIA Guide. We will take corrective action to ensure that the remaining four are updated.

Recommendation 27 *(Rolled-Forward from 2009)*

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 the OCIO.

The CIO does not concur with this recommendation and believes that all PIAs were reviewed by system owners in FY2011.

Recommendation 28 (*Rolled-Forward from 2008*)
We recommend that OPM continue its efforts to eliminate the unnecessary use of SSNs in accordance with OMB Memorandum M-07-16.

The CIO concurs with this recommendation and offers the following clarifying remarks. OPM currently does not have the funding to effectively pursue the elimination of unnecessary use of SSN's as stated in OMB memorandum M-07-16. Efforts are made when the unnecessary use of SSN is discovered in PTA and PIA documentation and efforts are explored with the program office for alternatives. OPM does comply with the requirement to meet regularly with other federal agencies on this effort.

Recommendation 29 (*Rolled-Forward from 2009*)
We recommend OPM incorporate Federal Acquisition Regulation 2007-004 language in all contracts related to common security settings.

The CIO concurs with this recommendation and will take the necessary corrective action.