



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 2012

Report No. 4A-CI-00-12-016

Date: 11/05/12

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

FEDERAL INFORMATION SECURITY
MANAGEMENT ACT AUDIT

FY 2012

WASHINGTON, D.C.

Report No. 4A-CI-00-12-016

Date: 11/05/12



Michael R. Esser
Assistant Inspector General
for Audits

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

FEDERAL INFORMATION SECURITY
MANAGEMENT ACT AUDIT

FY 2012

WASHINGTON, D.C.

Report No. 4A-CI-00-12-016

Date: 11/05/12

This final audit report documents the Office of Personnel Management's (OPM's) continued efforts to manage and secure its information resources.

The Office of the Chief Information Officer (OCIO) has recently made noteworthy improvements to OPM's IT security program. The OCIO has increased staffing levels in its IT Security and Privacy Group, and has had a stable Chief Information Security Officer for the past two and a half years. The OCIO has also successfully addressed a significant number of long-standing IT audit recommendations. However, it is clear that there are still opportunities for improvement in the overall management of OPM's IT security program.

In FY 2007 and FY 2008, we reported a material weakness in controls over the development and maintenance of OPM's IT security policies. In FY 2009, we expanded the material weakness 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, the OCIO updated its IT security and privacy policies, but made little progress in

addressing our concerns with OPM's security management structure. Throughout FY 2012, the OCIO continued to operate with a decentralized IT security structure that did not have the authority or resources available to adequately implement the new policies.

In August 2012, the OPM Director issued a memo to Associate Directors and Office Heads notifying them that IT security responsibilities would be centralized under the OCIO effective October 1, 2012. The OCIO has begun hiring IT security professionals to manage the security of OPM's major information systems. Once this transition is fully complete, we expect to close the audit recommendations related to IT security governance and remove the material weakness. However, the material weakness remains open in this report, as the agency's IT security function remained decentralized throughout the FY 2012 FISMA reporting period and because of the continuing instances of non-compliance with FISMA requirements.

The OCIO's response to our draft audit report indicated that they disagree with the classification of the material weakness because of the progress that OPM has made with its IT security program and because there was no loss of sensitive data during the fiscal year. However, the OCIO's statement is inaccurate, as there were in fact numerous information security incidents in FY 2012 that led to the loss or unauthorized release of mission-critical or sensitive data. Several of these security incidents were reported by the media. In addition, these incidents led to financial loss to the agency in the form of credit monitoring services paid for individuals affected by OPM's loss of their sensitive data.

In FY 2010, we added a second material weakness related to the management of the Certification and Accreditation process (now referred to as Security Assessment and Authorization or Authorization). In FY 2011, the OCIO improved its Authorization policies and templates, and added additional resources to facilitate the Authorization process. These improvements warranted reducing the material weakness related to Authorizations to a significant deficiency in the FY 2011 FISMA report. In FY 2012, we observed continued improvement in the OCIO's management of the Authorization process, and no longer consider this issue to be a significant deficiency.

In addition to the issues 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 OCIO has implemented an agency-wide information system configuration management policy and has established configuration baselines for all operating platforms used by the agency. However, Oracle databases are not routinely scanned for compliance with configuration baselines.
- The OCIO routinely conducts vulnerability scans of production servers, and has improved its capability to track outstanding vulnerabilities. However, the OCIO has not documented accepted weaknesses for servers or databases.

- The OCIO has implemented a process to apply operating system patches on all devices within OPM's network on a weekly basis. However, third party application patches are not applied in a timely manner.
- The OCIO has developed thorough incident response capabilities, but does not have a centralized network security operations center to continuously monitor security events.
- 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 specialized security training for individuals with information security responsibility could be improved.
- Plans of Action and Milestones (POA&M) exist for all information systems in OPM's inventory. However, several OPM systems have POA&M weaknesses that are significantly overdue and do not identify the resources required to correct the problem.
- The OCIO enforces the use of two-factor authentication for remote access, but VPN sessions do not terminate after 30 minutes of inactivity.
- OPM is not compliant with OMB Memorandum M-11-11, as no OPM systems require two-factor authentication using PIV credentials.
- The OCIO does not have the ability to detect unauthorized devices connected to the OPM network.
- The OCIO has taken steps toward implementing a continuous monitoring program at OPM; however, this project remains a work in progress.
- The IT security controls were adequately tested for only 34 of 47 information systems in OPM's inventory.
- The contingency plans were adequately tested for only 39 of 47 information systems in OPM's inventory.
- There is not a coordinated contingency plan/disaster recovery test between OPM's various general support systems.
- OPM program offices did not provide adequate oversight over contractors that operate information systems on behalf of the agency.
- OPM maintains an adequate security capital planning and investment program for information security.
- OPM is continuing its efforts to reduce the unnecessary use of Social Security Numbers.

Contents

Page

Executive Summary	i
Introduction	1
Background	1
Objectives	1
Scope and Methodology	2
Compliance with Laws and Regulations	3
Results	4
I. Information Security Governance	4
II. Security Assessment and Authorization	7
III. Risk Management	8
IV. Configuration Management	9
V. Incident Response and Reporting	12
VI. Security Training	14
VII. Plan of Action and Milestones	15
VIII. Remote Access Management	17
IX. Identity and Access Management	18
X. Continuous Monitoring Management	20
XI. Contingency Planning	22
XII. Contractor Systems	24
XIII. Security Capital Planning	25
XIV. Follow-up of Prior OIG Audit Recommendations	26
Major Contributors to this Report	27

Appendix I: The Office of the Chief Information Officer's October 16, 2012 comments on the draft audit report, issued September 27, 2012.

Appendix II: FY 2012 Inspector General FISMA reporting metrics

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 audit of OPM's security program and practices. As part of our audit, 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 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) 2012 Inspector General FISMA Reporting Instructions. This document provides a consistent form and format for agencies to report FISMA audit results 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;
- 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 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

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 2012.

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:

- Local Area Network / Wide Area Network General Support System (Report No. 4A-CI-00-12-014);
- Audit Report & Receivables Tracking System (Report No. 4A-OP-00-12-013); and
- Service Credit Redeposit and Deposit System (Report No. 4A-CF-00-12-015).

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 2012 Inspector General Federal Information Security Management Act Reporting Instructions;
- OPM Information Technology Security and Privacy 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, 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 2012 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 2012 FISMA audit of OPM's IT Security Program. Many recommendations were issued in prior FISMA audits and are rolled forward from the 2011 FISMA audit (Report no. 4A-CI-00-11-009).

I. Information Security Governance

In FY 2007 and FY 2008, we reported a material weakness in controls over the development and maintenance of OPM's IT security policies. In FY 2009, we expanded the material weakness 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, the OCIO updated its IT security and privacy policies, but made little progress in addressing our concerns with OPM's security management structure.

In August 2012, the OPM Director issued a memo mandating the transfer of IT security duties from the decentralized program office Designated Security Officers to a centralized team of Information System Security Officers (ISSO) that report to the OCIO. Once this transition is fully complete, we expect to close the audit recommendations related to IT security governance and remove the material weakness. However, the material weakness remains open in this report, as the agency's IT security function remained decentralized throughout the FY 2012 FISMA reporting period and because of the continuing instances of non-compliance with FISMA requirements.

The sections below provide additional details from the OIG's review of IT security governance at OPM.

a) Information Security Management Structure

Information system security at OPM has historically been managed by individual DSOs that report to the various program offices that own major computer systems.

In recent years, the OCIO has added resources to its IT Security and Privacy Group (headed by the Chief Information Security Officer or CISO) in an effort to improve oversight over DSO activity. However, the agency's security function continued to be ineffective, as 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. In addition, the CISO had no direct managerial leverage over the DSO community, and did not have the authority to require them to adhere to basic FISMA mandates such as conducting contingency plan and security controls tests on their systems.

It has been our long-standing opinion that OPM's approach to IT security is too decentralized. We recommended that OPM program offices should continue to have responsibility for developing, operating, and maintaining the information systems that

they own, but the DSO duties of documenting, testing, and monitoring information system security should be centralized within the OCIO.

In FY 2012, OPM took significant action to centralize its IT security function. OPM's Director issued a memorandum that transfers the DSO's security responsibility to the newly created ISSO role, effective October 1, 2012. By the end of FY 2012, the OCIO had filled three ISSO positions and assigned security responsibility for 17 of the agency's 47 information systems to these individuals. The OCIO intends to hire enough ISSOs to manage the security of all 47 systems.

While these actions are clearly positive steps that OPM has taken to centralize its IT security structure, the effort is not yet complete. The ISSOs have not yet performed any tangible security work for the systems they manage, and there are still many OPM systems that have not been assigned to an ISSO. Therefore, the material weakness remains in place for FY 2012, but we are optimistic that the OCIO's planned actions will lead to the closure of the audit recommendation and removal of the material weakness in FY 2013.

Recommendation 1 (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 CISO. 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 CISO should consist of experienced information security professionals.

OCIO Response:

“A CIO initiated Memo directing the centralization of the security responsibilities of Designated Security Officers (DSO) in the Office of Chief Information Security Officer (CISO) was issued by the OPM Director on August, 2012 with an effective date of October 1, 2012. The CIO has already hired staff with professional IT security experience and certifications. The initial set of systems have been transition[ed] to ISSOs for security management and we expect to have all OPM systems under CISO management once the full complement of professional security staff is on board and reporting to the CISO. We have also developed and delivered a communication plan to program offices and DSOs at a meeting held on September 26, 2012. The centralization of information security governance structure is underway under the CISO leadership.”

The OCIO's response also states that they disagree with the classification of this issue as a material weakness for the following reasons:

- 1. “A significant decision was made by the OPM Director in 2012 to consolidate all OPM IT resources under the OCIO. . . .*
- 2. Many of the findings mentioned have valid plans in motion . . . the IG should take into account the competing OPM priorities and the government wide*

reduction of operating funds available to address these which elongated many of the plans. . . .

3. *[There was] no financial or PII loss.”*

OIG Reply:

Although the OPM Director has approved the consolidation of IT resources under the CIO, this initiative is not complete. The OCIO has only taken over the security responsibility for approximately one-third of the agency’s major information systems, and does not currently have the qualified staff in place to take over the rest.

We continue to classify the problems associated with OPM’s information security governance as a material weakness because the efforts completed to date have clearly not yet improved the security posture of the agency to a satisfactory level. The findings in this audit report highlight the many instances of non-compliance with FISMA requirements that have been recurring at OPM for many years.

Contrary to the OCIO’s statement that there was no financial or PII loss in FY 2012, there were, in fact, numerous information security incidents that led to the loss or unauthorized release of mission-critical or sensitive data. Several of these security incidents were reported by the media. In addition, these incidents led to financial loss to the agency in the form of credit monitoring services paid for individuals affected by OPM’s loss of their sensitive data.

We do recognize the fact that the OCIO has valid plans in motion to address OPM’s IT security governance issues. However, a government-wide reduction of operating funds has no impact on the fact that this issue represents a material weakness that will continue to have negative consequences for the agency until it is fully addressed. We continue to recommend that the OPM Director provide the OCIO with the financial and administrative support that it needs to fully implement a centralized information security governance structure at OPM.

b) IT Security Policies and Procedures

OPM’s failure to adequately update its IT security and privacy policies and procedures was identified as a material weakness in the agency’s IT security program over the course of several FISMA audit reports.

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

- Information Security and Privacy Policy Handbook;
- Information Technology Security FISMA Procedures; and,
- OPM Security Assessment and Authorization Guide.

In FY 2012, the OCIO added an addendum to the Policy Handbook that addressed topics that we reported as missing from the original policy, including:

- Policy and procedures related to oversight of systems operated by a contractor;
- Policy on agency-wide risk management;
- 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.

The creation of these documents was sufficient to close our audit recommendations related to policies and procedures. However, the creation of policies and procedures alone does not improve an IT security program. They must be fully implemented by individuals with IT security responsibility. Given the longstanding issues with the decentralized structure of OPM's IT security program, we do not believe that the new policies can be effective until the centralized ISSO structure described above is fully implemented.

II. Security Assessment and Authorization

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 is referred to as Security Assessment and Authorization (Authorization).

Our FY 2008 and FY 2009 FISMA audit reports stated that weaknesses in OPM's Authorization 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 Authorization 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.

In FY 2011, the OCIO published updated procedures and templates designed to improve the overall Authorization process and dedicated resources to facilitating system Authorizations. We observed an improvement in the Authorization packages completed under this new process, and believed that this improvement warranted reducing the material weakness related to Authorization to a significant deficiency in the FY 2011 FISMA report.

In FY 2012, we observed a continued improvement in the Authorization packages completed under this new process. We reviewed the full Authorization packages of 12 systems that were subject to an Authorization during FY 2012. The quality of all packages appeared to be an improvement over Authorizations completed in prior years, and the packages present a more uniform approach to IT security from the OPM systems. As a result, we no longer consider this issue to be a significant deficiency in OPM's IT program.

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.”

In FY 2011, the OCIO organized a Risk Executive Function comprised of several IT security professionals. However, as of the end of FY 2012, the 12 primary elements of the Risk Executive Function as described in NIST SP 800-39 are still not all fully implemented. Key elements still missing from OPM’s approach to managing risk at an agency-wide level include: conducting a risk assessment, maintaining a risk registry, and communicating the agency-wide risks to the system owners.

Although the OCIO has made improvements in assessing risk at the individual system level (see Security Assessment and Authorization section II, above), the OCIO is not currently managing risk at an organization-wide level.

Recommendation 2 (Rolled-Forward from 2011)

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 Risk Executive Function will have agency wide authority and responsibility for assessing risk across all OPM lines of business. This position will not be

specific to the CIO or IT functions. The CIO has been seeking advice from the OIG on where the Risk Executive Function should report in the OPM organization and are pending a response.”

OIG Reply:

NIST SP 800-39 requires agencies to conduct an agency-wide risk assessment, maintain a risk registry, and communicate the agency-wide risks to the system owners. We have not received any evidence that the OCIO has implemented any of these requirements. We will provide feedback on the OCIO’s approach in addressing this recommendation, but it would be inappropriate for an OIG to design controls on behalf of management. We continue to recommend that the OCIO develop its Risk Executive Function to meet all of the requirements of the NIST guide.

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. However, many systems are not subject to adequate ongoing assessments of security controls (see section X(c) below).

IV. Configuration Management

The sections below detail the controls that the OCIO has in place to manage the technical configuration of OPM servers and workstations.

a) Agency-wide security configuration policy

OPM’s Information Security and Privacy Policy Handbook contains policies and procedures related to agency-wide configuration management. The handbook requires the establishment of secure baseline configurations and the monitoring and documenting of all configuration changes.

b) Configuration Baselines

In FY 2012, OPM put forth significant effort to document and implement new baseline configurations for servers, databases, and workstations. At the end of the fiscal year, the OCIO had established baselines and/or build sheets for the following

operating systems:

- Windows Server 2003;
- Windows Server 2008;
- Oracle; and
- Microsoft SQL Server.

The new baseline for the Linux operating platform is currently in development; we will follow up on the status of this item during the FY 2013 FISMA audit.

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

OPM user workstations are built with a standard image that is compliant with either the Federal Desktop Core Configuration (for Windows XP) or the United States Government Baseline Configuration (for Windows 7).

We conducted an automated scan on the Windows XP and Windows 7 standard images to independently verify compliance with the appropriate guideline. Nothing came to our attention to indicate that there are weaknesses in OPM's methodology to securely configure user workstations.

d) Compliance with Baselines

The OCIO uses automated scanning tools to conduct routine compliance audits on the majority of operating platforms used in OPM's server environment. These tools compare the actual configuration of servers and workstations to the approved baseline configuration. However, this routine audit is not currently performed for Oracle databases, which are only evaluated for compliance with the baseline a single time at the point of implementation.

NIST SP 800-53 Revision 3 control CM-3 requires agencies to audit activities associated with information system configurations.

Recommendation 3

We recommend that the OCIO implement a process to routinely audit Oracle databases for compliance with the approved OPM baseline configuration.

OCIO Response:

“OCIO has been working to standardize all operating systems and applications throughout the environment. Over the past year, all Windows and Linux operating systems, as well as Microsoft SQL have been given approved baseline images. Compliance scanning and configuration monitoring has also been established for these applications.”

OIG Reply:

Our report states that the OCIO conducts compliance audits on the “majority of operating platforms used in OPM’s server environment.” We acknowledge that this includes Windows, Linux, and Microsoft SQL Server. However, the audit finding is specific to Oracle databases, which the OCIO does not currently audit and did not address in its response. We continue to recommend that the OCIO implement a process to routinely audit Oracle databases for compliance with the approved OPM baseline configuration.

e) Software and Hardware Change Management

The OCIO has developed a Configuration Change Control Policy that outlines a formal process to approve and document all computer software and hardware changes.

We reviewed evidence indicating that the OCIO is adequately following this policy and is thoroughly documenting all system changes. Nothing came to our attention to indicate that there are weaknesses in OPM’s change management process.

f) Vulnerability Scanning

OPM’s Network Management Group (NMG) performs monthly vulnerability scans of all servers using automated scanning tools. A daily security advisory report is generated that details the most vulnerable servers and workstations; these reports are sent to system owners so they can remediate the identified weaknesses. The OCIO has improved its capability to accurately track all outstanding vulnerabilities and as a result, is able to remediate weaknesses in a timely manner.

NMG has documented accepted weaknesses for OPM user workstations; however, it has not fully documented weaknesses for servers or databases (i.e., vulnerability scan findings that are justified by a business need). This recommendation remains open and is rolled forward in FY 2012.

Recommendation 4 (Rolled-Forward from 2011)

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

OCIO Response:

“OCIO does not concur with this finding. This finding was addressed and has been accepted for closure.”

OIG Reply:

This recommendation has not been accepted for closure by either the OIG or the OPM audit follow-up office, Internal Oversight and Compliance (IOC). This recommendation remains open, and we advise the OCIO to review its records to

determine whether it has inappropriately classified the status of any other audit recommendations.

g) Patch Management

The OCIO has implemented a process to apply operating system patches on all devices within OPM's network on a weekly basis. We conducted vulnerability scans on a sample of servers and determined that servers are appropriately patched. However, our scans also determined that third party applications (i.e., Adobe, Java, etc.) on production servers are not adequately patched. The OCIO is currently working to develop a process to manage patches for third party applications.

NIST SP 800-53 Rev 3 control SI-2 requires the prompt installation of application patches, service packs, and hot fixes.

Recommendation 5

We recommend that the OCIO implement a process to timely patch (or remove altogether) third party applications on its servers.

OCIO Response:

“OCIO over the past year has reached out to the vendor of the patch management application and a project was developed to define, research, and select a solution to resolve this issue. A product has been selected and efforts are underway to implement this solution.”

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO continue to update IOC with its progress in implementing this recommendation.

V. Incident Response and Reporting

OPM's "Incident Response and Reporting Guide" outlines the responsibilities of OPM's Situation Room 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. OPM reiterates the information provided in the Incident Response and Reporting Guide in an annual mandatory IT security and privacy awareness training

course. In addition, OPM also uses three different software tools to prevent and detect intrusions and malware in the agency's network.

While the OCIO has processes in place to quickly respond to all **reported** security incidents, we are aware of several incidents that were not appropriately reported to the Situation Room in FY 2012. We conducted a separate audit related to these incidents and recommended that the OCIO conduct improved agency-wide training and implement additional awareness campaigns related to incident response (see OIG Report No. 4A-RI-00-12-033.) The OCIO provided documentation towards the end of the fiscal year indicating that it has improved the annual training. We will determine if the updated training material has improved incident response reporting as part of the FY 2013 FISMA audit.

b) Reporting incidents to US-CERT and law enforcement

OPM's Incident Response and Reporting policy states that OPM's Situation Room 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.

The Incident Response and Reporting policy also states that security incidents should be reported to law enforcement authorities, where appropriate. The OIG's Office of Investigations is part of the incident response notification distribution list, and is notified when security incidents occur.

c) Correlating and Monitoring Security Incidents

OPM owns a software product with the technical ability to compare and correlate security incidents over time. However, the correlation features of these tools are not being actively utilized at this time. This tool only receives event data from approximately 20 percent of all major OPM systems and is only being monitored during normal business hours. Furthermore, OPM does not have a consistent and unified process to monitor and analyze all security incidents. Some incidents cannot be fully investigated due to inconsistent logging practices across systems, and inefficiencies created by program offices running separate monitoring tools on their systems.

The OCIO's NMG is in the process of establishing an Enterprise Network Security Operations Center (ENSOC) that will provide continuous centralized support for OPM's security incident prevention/management, performance analysis, fault resolution, maintenance coordination, configuration management, security management, system monitoring, network monitoring, alert escalation, problem resolution bridge coordination, and incident response. Although we agree that the proposed ENSOC will greatly improve OPM's incident management capabilities, the OCIO continues to face resource limitations that hinder the full implementation of the ENSOC.

Recommendation 6

We recommend that the OCIO establish a centralized network security operations center with the ability to monitor security events for all major OPM systems.

OCIO Response:

“A centralized monitoring center is being established with first level alerting and monitoring for the servers, and network appliances within the major OPM sites. Work has begun on incorporating application and database monitoring and compliance. OCIO deferred investment in a final solution to allow for an enterprise wide one after a data center relocation effort is completed in FY13.”

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO continue to update IOC with its progress in implementing this recommendation.

VI. Security Training

FISMA requires all government employees and contractors 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 98 percent of OPM’s employees and over 95 percent of contractors completed the security awareness training course in FY 2012.

b) Specialized IT security training

OPM 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. 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 86 percent have completed the required specialized security training in FY 2012.

Recommendation 7 (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:

“Significant improvements were achieved this year with a completion rate of over 85 percent taking specialize[d] security training compared with approximately 75 percent in FY 2011. We plan to resubmit additional training information before this report is finalized for a number of users whose initial submissions were rejected. We expect the resubmissions to result in a completion rate of over 94 percent.”

OIG Reply:

We did not receive a resubmission of the security training results from the OCIO, and only have evidence supporting an 85 percent compliance rate. Although this does represent an improvement over the prior year, the OCIO has not fully met this basic FISMA requirement for the past three years. We will test 2013 security training compliance as part of next year’s FISMA audit.

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. 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 November 2011, the OIG issued the FY 2011 FISMA audit report with 29 audit recommendations. We verified that all 29 of the recommendations were appropriately incorporated into the OCIO master POA&M.

Although only 34 of OPM’s 47 major systems were subject to annual security controls tests (see section X, below), we were able to verify that all security weaknesses identified during these tests were incorporated into the appropriate system’s POA&M.

b) Prioritize Weaknesses

Each program office at OPM is required to prioritize the security weaknesses on their POA&Ms to help ensure significant IT issues are addressed in a timely manner. We verified that the POA&Ms for all 47 OPM systems identified the prioritization of each security weakness.

c) Effective Remediation Plans and Adherence to Remediation Deadlines

All system owners are required to create action steps (milestones) to effectively remediate specific weaknesses identified on POA&Ms. Our review of the POA&Ms indicated that system owners are appropriately listing milestones and target completion dates on their POA&Ms.

However, our review also indicated that many system owners are not meeting the self-imposed remediation deadlines listed on the POA&Ms. Twenty-two of OPM's 47 systems have POA&M items that are greater than 120 days overdue. We issued an audit recommendation in FY 2010 related to overdue POA&M items. This recommendation was closed in FY 2011 because there were significant improvements in the number of overdue POA&M items. However, the regression identified in FY 2012 requires us to re-issue this recommendation.

Recommendation 8

We recommend that the OCIO and system owners develop formal corrective action plans to remediate all POA&M weaknesses that are over 120 days overdue.

OCIO Response:

“The CIO dedicated resources to this task and has successfully closed almost all of the POA&Ms that are over 120 [days overdue] and will continue to work with program offices to close those that are outstanding. Most POA&Ms that are over 120 days have dependencies such as funding that is not available or coordination issues with external entities who often are not ready to implement the required changes.”

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO provide IOC with evidence that it has closed “almost all” POA&Ms that are over 120 days overdue. Once received, IOC and the OIG will promptly review this evidence and consider this recommendation for closure.

d) Identifying Resources to Remediate Weaknesses

We interviewed the DSOs for 10 of the systems with overdue POA&M items. Each DSO stated that although they have identified the resources required to address the POA&M items, these resources are not currently available.

We also noted that 11 POA&Ms have not identified the resources that would be required to address POA&M weaknesses, as required by OPM's POA&M policy.

Recommendation 9

We recommend that all POA&Ms list the specific resources required to address each security weakness identified.

OCIO Response:

“Work has started to ensure that POA&Ms are updated to include the ‘resources required’ information and we expect to make steady progress in FY13. We will continue to work with program offices to ensure that the resources required for POA&Ms are identified.”

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO continue to update IOC with its progress in implementing this recommendation.

e) OCIO tracking and reviewing POA&M activities on a quarterly basis

The OCIO requires program offices to provide the evidence, or “proof of closure,” that security weaknesses have been resolved before officially closing the related POA&M. When the OCIO receives a proof of closure document from the program offices for a POA&M item, an OCIO employee will judgmentally review the documentation to determine whether or not the evidence provided was appropriate.

We selected one closed POA&M item from 10 OPM 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 the 47 OPM systems and were judgmentally chosen by OIG auditors. We determined that adequate proof of closure was provided for all 10 systems tested. The results of the sample test were not projected to the entire population.

VIII. Remote Access Management

OPM has implemented policies and procedures related to authorizing, monitoring, and controlling all methods of accessing the agency’s network resources from a remote location. In addition, OPM has issued agency-wide telecommuting policies and procedures, and all employees are required to sign a Rules of Behavior document that outlines their responsibility for the protection of sensitive information when working remotely.

OPM utilizes a Virtual Private Network (VPN) client to facilitate secure remote access to the agency’s network environment. The OPM VPN requires the use of an individual’s PIV card and password authentication to uniquely identify users. OIG has reviewed the VPN access list to ensure that there are no shared accounts and that each user account has been tied to an individual. The agency maintains logs of individuals who remotely access the network, and the logs are reviewed on a monthly basis for unusual activity or trends.

Although there are still a small portion of authorized network devices that are not compliant with PIV cards (e.g., iPad), these devices still require multi-factor authentication for remote access through the use of RSA tokens and password authentication.

We did note one problem related to the FISMA requirement that a remote access session be terminated or locked out after 30 minutes of inactivity. We connected two workstations to OPM's VPN server and left them idle for over 1 hour, but neither VPN session was terminated during this time.

Recommendation 10

We recommend the OCIO configure the VPN servers to terminate VPN sessions after 30 minutes of inactivity.

OCIO Response:

“All technological controls are in place and OCIO believes this is a major flaw in a vendor's design that will require an out of band patch to repair. OCIO is in the process of implementing secondary controls to mitigate this issue until the patch is released. OCIO has narrowed [the] problem to a fault within the UDP connection to the client and are working with Cisco to get this resolved.”

OIG Reply:

As of the issuance of this report, idle VPN sessions can remain connected indefinitely. As part of the audit resolution process, we recommend that the OCIO continue to update IOC with its progress in implementing this recommendation.

IX. Identity and Access Management

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

a) Policies for Account and Identity Management

OPM maintains policies and procedures for agency-wide account and identity management within the OCIO Information Security and Privacy Policy Handbook. The policies contain procedures for creating user accounts with the appropriate level of access as well as procedures for removing access for terminated employees.

b) Terminated Employees

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.

In the FY 2011 FISMA audit there were two recommendations related to OPM's failure to remove LAN access for terminated employees. In response, the OCIO implemented a process to routinely audit all active user accounts to search for terminated employees or duplicate accounts.

c) Multi-Factor Authentication with PIV

OMB Memorandum M-11-11 required all federal information systems to be upgraded to use PIV credentials for multi-factor authentication by the beginning of FY 2012. In addition, the memorandum stated that all new systems under development must be PIV compliant prior to being made operational, and that agencies must be compliant with the memorandum prior to using technology refresh funds to complete other activities.

In FY 2012, the OCIO began an initiative to require PIV authentication to access the agency's network; the project is scheduled to be completed in January 2013. However, as of the end of the FY 2012, none of the 47 major systems at OPM require PIV authentication.

Recommendation 11

We recommend that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.

OCIO Response:

“OPM has achieved 100% PIV usage for all remote connections and are implementing PIV usage within the OPM population based on its current project plan. OCIO plans to have to achieve 50% compliance by Q3 FY13.”

OIG Reply:

The OCIO's response to this recommendation leads us to believe that it does not fully understand the requirements of OMB M-11-11. The memorandum requires each major application to enforce two-factor authentication via PIV credentials. PIV usage for remote connections or access to the network environment does not address this requirement. As of the issuance of this report, OPM has 0 percent compliance with OMB M-11-11, and we continue to recommend that OPM upgrade its major information systems to require multi-factor authentication using PIV credentials.

d) Unauthenticated Network Devices

Since FY 2010 we have recommended that the OCIO implement an automated process to detect non-approved devices connected to OPM's network. The OCIO has recently purchased a Network Access Controller (NAC) that will govern access to network resources. The NAC has the ability to identify all devices on the network and deny access to unrecognized devices. However, as of the end of FY 2012, the NAC has not been installed and configured for use at OPM.

Recommendation 12 (Rolled-Forward from 2010)

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

OCIO Response:

“The network detection solution is in place and continued enforcement of NAC was delayed due to unforeseen vendor faults. OCIO, with the vendor, has developed remediation steps and this project will be completed on schedule (Q3 FY13).”

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO continue to update IOC with its progress in implementing this recommendation.

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 to ensure continued effectiveness. In FY 2012, the OCIO published an addendum to the Information Security and Privacy Policy which states that it is the ISSO/DSOs responsibility to assess all security controls in an information system. As stated above in section I, the ISSO function has not been fully established at OPM. Our FY 2011 FISMA report stated that many of the current DSOs do not have the technical skills or the resources required to adequately monitor the information security controls of their systems. Therefore, we believe that OPM’s continuous monitoring policies and procedures cannot be adequately implemented until the agency’s centralized ISSO function has been fully established.

b) Continuous Monitoring Strategy

The OCIO developed a concept of operations document and a continuous monitoring program implementation “roadmap” that describes the stages and timeline for implementing a full continuous monitoring program at OPM. While the initial stages of implementation began in FY 2012, full implementation of the plan is not scheduled to be completed until FY 2014. The next stage in the OCIO’s plan involves system owners evaluating specific security controls on an increasingly frequent basis. Implementation of this stage is scheduled to be completed during FY 2013.

Recommendation 13

We recommend that the OCIO expand its continuous monitoring program to include a reporting process at the system-level, and implement automated tools and metric reporting for OPM as outlined in the Information Security Continuous Monitoring Roadmap.

OCIO Response:

“A comprehensive continuous monitoring plan was developed and briefed to the OIG and KPMG in 2012. The plan calls for a 4 phase implementation approach and we have started phase 1 implementation. Each system now has its own continuous monitoring plan and we expect to fully implement the phases of the continuous monitoring road map in FY2013.”

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO continue to update IOC with its progress in implementing this recommendation.

c) Annual Assessment of Security Controls

Although OPM has begun implementing a continuous monitoring approach to information security controls, FISMA still requires information system owners to assess security controls on an annual basis.

We requested the annual security controls test results for all OPM systems in order to review them for quality and consistency. However, we were only provided testing documentation for 34 out of the 47 major systems at OPM. Of the tests we did receive, the quality varied considerably. 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 has traditionally placed responsibility on the various program offices to test the security controls of their systems. The OCIO’s lack of authority over these program offices has contributed to the inadequate security controls testing of the agency’s information systems. We also believe that the DSO’s lack of technical skills also contributes to the problem. It has been over four years since all OPM systems were subject to an annual security controls test. We are optimistic that the quality and consistency of security controls tests will improve with the implementation of the OCIO’s centralized ISSO structure.

Recommendation 14 (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 made significant progress with security controls testing in FY2012. We plan to implement continuous monitoring with professional security staff reporting to the CISO. The security staff will have the lead responsibility for continuous monitoring of OPM systems. Annual security controls testing will be included in the continuous monitoring program.”

OIG Reply:

We do not agree that the OCIO has made significant progress with security controls testing in FY 2012. In fact, the 2012 compliance rate of 72 percent is a regression from the 2011 rate of 75 percent. OPM's failure to meet this basic FISMA requirement for the past five years is a major contributing factor to our classification of information security governance as a material weakness. We will evaluate the FY 2013 compliance rate as part of next year's FISMA audit.

XI. Contingency Planning

OPM's Information Security Privacy and Policy Handbook requires a contingency plan to be in place for each information system and that each system's contingency plan be tested on an annual basis. The sections below detail our review of contingency planning activity in FY 2012.

a) Documenting contingency plans of individual OPM systems

We verified that contingency plans exist for all 47 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.

b) Testing contingency plans of individual OPM systems

OPM's Information Security Privacy and Policy Handbook requires that the contingency plan for each information system be tested at least annually using information system specific tests and exercises. However, we received evidence that contingency plans were tested for only 39 of 47 systems in FY 2012.

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.

The OCIO has issued detailed guidance to program offices on how to conduct a contingency plan test and create an after action report. Our reviews have indicated that the program office DSOs currently responsible for conducting the contingency plan tests do not have the technical experience to adequately perform the task. We expect that the new centralized security function will improve this weakness, as contingency plan tests will be performed by the ISSO security professionals.

Recommendation 15 (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 eight systems that were not subject to adequate testing in FY 2012.

OCIO Response:

“The CIO expects to make progress with contingency plan testing in [FY 2013]. It is expected that professional security staff reporting to the CISO will play a leading role in contingency plan testing.”

OIG Reply:

We will evaluate the FY 2013 compliance rate as part of next year's FISMA audit. If the centralized governance structure is fully implemented, we are optimistic that compliance with contingency plan testing requirements will show improvement.

c) Testing contingency plans of OPM general support systems

Many OPM systems reside on one of the agency's general support systems. The OCIO conducts a full recovery test of the Enterprise Server Infrastructure general support system (i.e., the mainframe and associated systems) on an annual basis. However, the LAN/WAN general support system is not subject to a full functional disaster recovery test on a routine basis. Only select LAN/WAN systems that impact or interface with the mainframe environment are tested annually in conjunction with the mainframe disaster recovery test.

In July 2012 a failure of the OPM data center's uninterruptable power supply led to the unavailability of e-mail, Internet, and major information systems for a significant period of time. According to OPM's disaster recovery plans, these critical services should have been instantly switched over to an alternate OPM processing site. We believe that routine functional disaster recovery testing of the LAN/WAN general support system can help prevent failures like this from occurring in the future.

NIST SP 800-53 Revision 3 states that FIPS 199 “high” systems should be subject to “a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.” Without full functional routine testing of all OPM general support systems, there is a risk that OPM systems will not be successfully recovered in the event of a disaster.

In the FY 2011 FISMA audit report we recommended that the OCIO implement a centralized (agency-wide) approach to contingency plan testing. We were informed that a single synchronized functional test is not feasible due to logistical and resource limitations. However, the intent of the recommendation is to ensure that all elements of the general support systems are subject to a full functional disaster recovery test each year. This recommendation can be remediated if each general support system is subject to a full functional test each year, even if it must be broken into a series of smaller tests.

Recommendation 16 (rolled forward from 2011)

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

OCIO Response:

“OCIO concurs with this finding and is taking steps to assign personnel to this responsibility. A project is in progress to fully map the applications and systems and software is being acquired to track and report the testing.”

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO continue to update IOC with its progress in implementing this recommendation.

XII. Contractor Systems

We evaluated the methods that the OCIO and various program offices use to maintain oversight of their systems operated by contractors on behalf of OPM.

1. Contractor System Documentation

OPM’s master system inventory indicates that 17 of the agency’s 47 major applications are operated by a contractor. The OCIO also maintains a separate spreadsheet documenting interfaces between OPM and contractor-operated systems and the related Interconnection Security Agreements.

2. Contractor System Oversight

The OPM Information Security and Privacy Policy Addendum states that “It is the responsibility of the OPM system owner to ensure systems or services hosted by non-OPM organizations comply with OPM information security and privacy policies.”

The OCIO distributes an annual Site Survey Assessment that program offices are required to complete for all contractor-operated systems. The survey requires the program office to document the physical, operational, organizational, and technical security controls in place at the contractor facilities.

Although the Site Survey Assessment is conceptually a good approach to overseeing contractor systems, the contractor is permitted to complete the survey themselves as opposed to an OPM employee or independent third party. We do not believe that this constitutes adequate independent oversight.

A control enhancement to the security assessment section of NIST SP 800-53 Revision 3 states that the agency “employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.” In our opinion, adequate oversight over contractor systems would require a federal employee or an independent third party to conduct the annual security controls tests as well as the triennial system Authorization.

Recommendation 17

We recommend that the OPM Information Technology Security and Privacy Handbook be updated to explicitly require contractor-operated systems to be subject to an annual security controls test performed by a government employee or an independent third party. The security controls tests should be documented using OPM’s standard templates.

OCIO Response:

“Comprehensive IT security & Privacy policies were developed and published in 2011 and a policy addendum with updated policies was published in 2012 and accepted by the OIG and KPMG. The new OIG’s policy recommendations will be added to existing policies in FY2013.”

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO continue to update IOC with its progress in implementing this recommendation.

XIII. Security Capital Planning

NIST SP 800-53 Revision 3 control 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 2011 were rolled forward into one of the recommendations in the FY 2011 OIG FISMA audit report (Report 4A-CI-00-11-009). FY 2011 recommendations that were not remediated by the end of FY 2012 are rolled forward with a new recommendation number in this FY 2012 OIG FISMA audit report.

The prior sections of this report evaluate the current status of many 2011 recommendations. However, there is one additional 2011 recommendation that has not yet been addressed in this report because the related topic was not part of the FY 2012 FISMA reporting instructions. The current status of this recommendation is below.

a) 4A-CI-00-11-009 Recommendation 28 (Rolled-Forward From 2008)

The OCIO has an ongoing plan to reduce and eventually eliminate the unnecessary use of SSNs in its major information systems. However, resource limitations prevented them from completing this task in FY 2012. This recommendation remains open and is rolled forward in FY 2012.

Recommendation 18 (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:

“Significant work was done to eliminate the unnecessary use of social security numbers (SSN) including development of a consolidated Action Plan. The CIO has also eliminated the use of SSNs in USAJOBS and the PMF systems. The CIO's policy is to not approve new IT systems that intend to use SSN unless related to payroll functions. In FY2013, we plan to issue additional guidance to program offices on the requirement to eliminate the unnecessary use of SSNs and will continue to work with program offices on this important recommendation.”

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO continue to update IOC with its progress in implementing this recommendation.

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

Appendix I



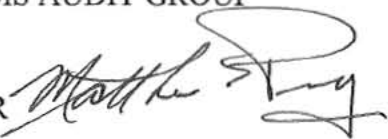
UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

Chief Information
Officer

OCT 16 2012

MEMORANDUM FOR: [REDACTED]
CHIEF, INFORMATION SYSTEMS AUDIT GROUP

FROM: MATTHEW E. PERRY
CHIEF INFORMATION OFFICER 

Subject: Response to the Federal Information Security Management Act Audit
FY 2012, Report NO.4A-CI-00-12-016

Thank you for the opportunity to comment on the subject report. We plan to continue making improvements in our security risk management strategy and the OPM IT security program.

Respectfully, OCIO does not agree though with the Material Weakness rating and submits it should be reduced to a Significant Deficiency. A number of factors weigh into our position:

- A significant decision was made by the OPM Director in 2012 to consolidate all OPM IT resources under the OCIO. This enabled the OCIO to have full authorities and reach into previously independent IT areas. The ability to centrally manage and review all IT components is a key improvement to OCIO's success in remediation of the findings;
- Many of the findings mentioned have valid plans in motion that show improvements and detail plans to complete the findings recommendations. OCIO feels the IG should take into account the competing OPM priorities and the government wide reduction of operating funds available to address these which elongated many of the plans;
- Working with the CFO and the Directors office, in FY 12, OCIO was provided reallocated funding to hire ISSO's and to implement solutions to many of these highly visible findings. Many of which are showing tangible success this past year, such as no financial or PII loss.

Finally, OCIO feels that OPM is in a much better security posture than the previous years based on the hard work and investment from management. This is reflected in the recent KPMG decision to lower their Material Weakness rating to a Significant Deficiency for this current audit year.

Again, respectfully, OCIO believes that this rating should be reduced based on the above.

OIG Recommendations:

Recommendation 1 (Rolled-Forward from 2010)

We recommend that OPM implement centralized information security governance structure where all information security practitioners, including designated security officers, report to the CISO. 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 CISO should consist of experienced information security professionals.

(OCIO does not concur)

A CIO initiated Memo directing the centralization of the security responsibilities of Designated Security Officers (DSO) in the Office of Chief Information Security Officer (CISO) was issued by the OPM Director on August, 2012 with an effective date of October 1, 2012. The CIO has already hired staff with professional IT security experience and certifications. The initial set of systems have been transition to ISSOs for security management and we expect to have all OPM systems under CISO management once the full complement of professional security staff is on board and reporting to the CISO. We have also developed and delivered a communication plan to program offices and DSOs at a meeting held on September 26, 2012. The centralization of information security governance structure is underway under the CISO leadership.

Recommendation 2 (Rolled-Forward from 2011)

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 does not concur)

The Risk Executive Function will have agency wide authority and responsibility for assessing risk across all OPM lines of business. This position will not be specific to the CIO or IT functions. The CIO has been seeking advice from the OIG on where the Risk Executive Function should report in the OPM organization and are pending a response.

Recommendation 3

We recommend that the OCIO implement a process to routinely audit Oracle Databases for compliance with the approved OPM baseline configuration.

(OCIO does not concur)

OCIO has been working to standardize all operating systems and applications throughout the environment. Over the past year, all Windows and Linux operating systems, as well as Microsoft SQL have been given approved baseline images. Compliance scanning and configuration monitoring has also been established for these applications.

Recommendation 4 (Rolled-Forward from 2011)

We recommend that the OCIO document “accepted” weaknesses identified in Vulnerability scans.

(OCIO does not concur)

OCIO does not concur with this finding. This finding was addressed and has been accepted for closure.

Recommendation 5

We recommend that the OCIO implement a process to timely patch (or remove altogether) third party applications on its servers.

(OCIO does not concur)

OCIO over the past year has reached out to the vendor of the patch management application and a project was developed to define, research, and select a solution to resolve this issue. A product has been selected and efforts are underway to implement this solution.

Recommendation 6

We recommend that the OCIO establish a centralized network security operations center with the ability to monitor security events for all major OPM systems.

(OCIO does not concur)

A centralized monitoring center is being established with first level alerting and monitoring for the servers, and network appliances within the major OPM sites. Work has begun on incorporating application and database monitoring and compliance. OCIO deferred investment in a final solution to allow for an enterprise wide one after a data center relocation effort is completed in FY13.

Recommendation 7 (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 does not concur)

Significant improvements were achieved this year with a completion rate of over 85 percent taking specialize security training compared with approximately 75 percent in FY 2011. We plan to resubmit additional training information before this report is finalized for a number of users whose initial submissions were rejected. We expect the resubmissions to result in a completion rate of over 94 percent.

Recommendation 8

We recommend that the OCIO and system owners develop formal corrective action plans to immediately remediate all POA&M weaknesses that are over 120 days overdue.

(OCIO concurs)

The CIO dedicated resources to this task and has successfully closed almost all of the POA&Ms that are over 120 day and will continue to work with program offices to close those that are outstanding. Most POA&Ms that are over 120 days have dependencies such as funding that is not available or coordination issues with external entities who often are not ready to implement the required changes. It is suggested that the word “immediate” be removed from recommendation 8 since immediate resolution is not feasible.

Recommendation 9

We recommend that all POA&Ms list the specific resources required to address each security weakness identified.

(OCIO Concur)

Work has started to ensure that POA&Ms are updated to include the “resources required” information and we expect to make steady progress in FY13. We will continue to work with program offices to ensure that the resources required for POA&Ms are identified.

Recommendation 10

We recommend the OCIO configure the VPN servers to terminate VPN sessions after 30 minutes of inactivity.

(OCIO does not concur)

All technological controls are in place and OCIO believes this is a major flaw in a vendor’s design that will require an out of band patch to repair. OCIO is in the process of implementing secondary controls to mitigate this issue until the patch is released. OCIO has narrowed problem to a fault within the UDP connection to the client and are working with Cisco to get this resolved.

Recommendation 11

We recommend that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.

(OCIO does not concur)

OPM has achieved 100% PIV usage for all remote connections and are implementing PIV usage within the OPM population based on its current project plan. OCIO plans to have to achieve 50% compliance by Q3 FY13.

Recommendation 12 (Rolled-Forward from 2010)

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

(OCIO does not concur)

The network detection solution is in place and continued enforcement of NAC was delayed due to unforeseen vendor faults. OCIO , with the vendor, has developed remediation steps and this project will be completed on schedule (Q3 FY13).

Recommendation 13

We recommend that the OCIO expand its continuous monitoring program to include a reporting process at the system-level, and implement automated tools and metric reporting for OPM as outlined in the Information Security Continuous Monitoring Roadmap.

(OCIO does not concur)

A comprehensive continuous monitoring plan was developed and briefed to the OIG and KPMG in 2012. The plan calls for a 4 phase implementation approach and we have started phase 1 implementation. Each system now has its own continuous monitoring plan and we expect to fully implement the phases of the continuous monitoring road map in FY2013.

Recommendation 14 (Rolled forward from 2008)

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

(OCIO concurs)

The CIO made significant progress with security controls testing in FY2012. We plan to implement continuous monitoring with professional security staff reporting to the CISO. The security staff will have the lead responsibility for continuous monitoring of OPM systems. Annual security controls testing will be included in the continuous monitoring program.

Recommendation 15 (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 2012.

(OCIO Concur)

The CIO expects to make progress with contingency plan testing in FY2012. It is expected that professional security staff reporting to the CISO will play a leading role in contingency plan testing.

Recommendation 16 (rolled forward from 2011)

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

(OCIO Concur)

OCIO concurs with this finding and is taking steps to assign personnel to this responsibility. A project is in progress to fully map the applications and systems and software is being acquired to track and report the testing.

Recommendation 17

We recommend that the OPM Information Technology Security and Privacy Handbook be updated to explicitly require contractor operated systems to be subject to an annual security controls test performed by a government employee or an independent third party. The security control tests should be documented using OPM's standard templates.

(OCIO Concur)

Comprehensive IT security & Privacy policies were developed and published in 2011 and a policy addendum with updated policies was published in 2012 and accepted by the OIG and KPMG. The new OIG's policy recommendations will be added to existing policies in FY2013.

Recommendation 18 (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 does not concur)

Significant work was done to eliminate the unnecessary use of social security numbers (SSN) including development of a consolidated Action Plan. The CIO has also eliminated the use of SSNs in USAJOBS and the PMF systems. The CIO's policy is to not approve new IT systems that intend to use SSN unless related to payroll functions. In FY2013, we plan to issue additional guidance to program offices on the requirement to eliminate the unnecessary use of SSNs and will continue to work with program offices on this important recommendation.

Inspector General

Section Report

2012

Annual FISMA
Report

Office of Personnel Management

Section 1: Continuous Monitoring Management

- 1.1 **Has the Organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:**

No

Comments:

OPM's Office of the Chief Information Officer (OCIO) developed a concept of operations document and a continuous monitoring program implementation "roadmap" that describes the stages and timeline for implementing a full continuous monitoring program at OPM. While the initial stages of implementation began in FY 2012, full implementation of the plan is not scheduled to be completed until FY 2014

- 1.1.1 **Documented policies and procedures for continuous monitoring (NIST 800-53: CA-7)**

Yes

- 1.1.2 **Documented strategy and plans for continuous monitoring (NIST 800-37 Rev 1, Appendix G)**

Yes

- 1.1.3 **Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST 800-53, NIST 800-53A)**

No

Comments:

Only 34 of OPM's 47 major applications were subject to any form of security controls testing in FY 2012.

- 1.1.4 **Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions and updates with the frequency defined in the strategy and/or plans (NIST 800-53, NIST 800-53A)**

Yes

- 1.2 **Please provide any additional information on the effectiveness of the Organization's Continuous Monitoring Management Program that was not noted in the questions above**

Continuous Monitoring

Comments:

OPM's decentralized approach to IT security has traditionally placed responsibility on the various program offices to test the security controls of their systems. The OCIO's lack of authority over these program offices has contributed to the inadequate security controls testing of the agency's information systems. We also believe that the program office's security personnel lack of technical skills contributes to the problem. It has been over four years since all OPM systems were subject to an annual security controls test. We are optimistic that the quality and consistency of security controls tests will improve with the planned reorganization and centralization of the agency's IT security program.

Section 2: Configuration Management

2.1 Has the Organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

2.1.1 Documented policies and procedures for configuration management

Yes

2.1.2 Standard baseline configurations defined

Yes

2.1.3 Assessing for compliance with baseline configurations

Yes

Comments:

OPM's OCIO uses automated scanning tools to conduct routine compliance audits on the majority of operating platforms used in OPM's server environment. These tools compare the actual configuration of servers and workstations to the approved baseline configuration. However, this routine audit is not currently performed for Oracle databases, which are only evaluated for compliance with the baseline a single time at the point of implementation.

2.1.4 Process for timely, as specified in Organization policy or standards, remediation of scan result deviations

Yes

2.1.5 For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented

Yes

2.1.6 Documented proposed or actual changes to hardware and software configurations

Yes

2.1.7 Process for timely and secure installation of software patches

Yes

Section 2: Configuration Management

2.1.8 Software assessing (scanning) capabilities are fully implemented (NIST 800-53: RA-5, SI-2)

No

Comments:

OPM's OCIO has improved its capability to accurately track all weaknesses identified in vulnerability scans and as a result, is able to remediate weaknesses in a timely manner. The OCIO has documented accepted weaknesses for OPM user workstations; however, it has not fully documented weaknesses for servers or databases (i.e., vulnerability scan findings that are justified by a business need).

2.1.9 Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in Organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)

Yes

2.1.10 Patch management process is fully developed, as specified in Organization policy or standards. (NIST 800-53: CM-3, SI-2)

Yes

Comments:

We conducted vulnerability scans on a sample of servers and determined that servers are appropriately patched. However, our scans also determined that third party applications (i.e., Adobe, Java, etc.) on production servers are not adequately patched. The OCIO is currently working to develop a process to manage patches for third party applications.

2.2 Please provide any additional information on the effectiveness of the Organization's Configuration Management Program that was not noted in the questions above.

Configuration Management

Section 3: Identity and Access Management

3.1 Has the Organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes:

Yes

3.1.1 Documented policies and procedures for account and identity management (NIST 800-53: AC-1)

Yes

Section 3: Identity and Access Management

3.1.2 Identifies all users, including federal employees, contractors, and others who access Organization systems (NIST 800-53, AC-2)

Yes

Comments: Since FY 2010 we have recommended that the OCIO implement an automated process to detect non-approved devices connected to OPM's network. The OCIO has recently purchased a Network Access Controller (NAC) that will govern access to network resources. The NAC has the ability to identify all devices on the network and deny access to unrecognized devices. However, as of the end of FY 2012, the NAC has not been installed and configured for use at OPM.

3.1.3 Identifies when special access requirements (e.g., multi-factor authentication) are necessary.

No

Comments: OPM has not yet documented which systems require special access requirements, as many systems are currently incompatible with PIV readers.

3.1.4 If multi-factor authentication is in use, it is linked to the Organization's PIV program where appropriate (NIST 800-53, IA-2)

No

Comments: See note in 3.1.5.

3.1.5 Organization has adequately planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11)

No

Comments: In 2012, OPM's OCIO began an initiative to require PIV authentication to access the agency's network; the project is scheduled to be completed in January 2013. However, as of the end of the FY 2012, none of the 47 major systems at OPM require PIV authentication, as required by OMB M-11-11.

3.1.6 Ensures that the users are granted access based on needs and separation of duties principles

Yes

3.1.7 Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users (For example: IP phones, faxes, printers are examples of devices attached to the network that are distinguishable from desktops, laptops or servers that have user accounts)

Yes

Section 3: Identity and Access Management

3.1.8 Identifies all User and Non-User Accounts (refers to user accounts that are on a system. Examples of non-user accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users)

Yes

3.1.9 Ensures that accounts are terminated or deactivated once access is no longer required

Yes

3.1.10 Identifies and controls use of shared accounts

Yes

3.2 Please provide any additional information on the effectiveness of the Organization's Identity and Access Management Program that was not noted in the questions above.

Identity and Access Management

Section 4: Incident Response and Reporting

4.1 Has the Organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

4.1.1 Documented policies and procedures for detecting, responding to and reporting incidents (NIST 800-53: IR-1)

Yes

4.1.2 Comprehensive analysis, validation and documentation of incidents

Yes

4.1.3 When applicable, reports to US-CERT within established timeframes (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)

Yes

4.1.4 When applicable, reports to law enforcement within established timeframes (SP 800-86)

Yes

Section 4: Incident Response and Reporting

4.1.5 Responds to and resolves incidents in a timely manner, as specified in Organization policy or standards, to minimize further damage. (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)

Yes

4.1.6 Is capable of tracking and managing risks in a virtual/cloud environment, if applicable

Yes

Comments: OPM has incident response policies and procedures that govern all systems, including those that reside in a cloud. However, OPM has not documented which systems reside in the cloud.

4.1.7 Is capable of correlating incidents

Yes

4.1.8 There is sufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)

No

Comments: OPM owns a software product with the technical ability to compare and correlate security incidents over time. However, the correlation features of these tools are not being actively utilized at this time. This tool only receives event data from approximately 20% of all major OPM systems and is only being monitored during normal business hours. Furthermore, OPM does not have a consistent and unified process to monitor and analyze all security incidents. Some incidents cannot be fully investigated due to inconsistent logging practices across systems, and inefficiencies created by program offices running separate monitoring tools on their systems.

4.2 Please provide any additional information on the effectiveness of the Organization's Incident Management Program that was not noted in the questions above.

Incident Response and Reporting

Section 5: Risk Management

Section 5: Risk Management

5.1 Has the Organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

No

Comments:

In FY 2011, the OCIO organized a Risk Executive Function comprised of several IT security professionals. However, as of the end of FY 2012, the 12 primary elements of the Risk Executive Function as described in NIST SP 800-39 are still not all fully implemented. Key elements still missing from OPM's approach to managing risk at an agency-wide level include: conducting a risk assessment, maintaining a risk registry, and communicating the agency-wide risks down to the system owners. Although the OCIO has made improvements in assessing risk at the individual system level (see Security Assessment and Authorization section II, above), the OCIO is not currently managing risk at an organization-wide level.

5.1.1 Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process

Yes

5.1.2 Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev.1

No

Comments:

See comment in 5.1.

5.1.3 Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev.1

Yes

5.1.4 Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1

Yes

5.1.5 Categorizes information systems in accordance with government policies

Yes

5.1.6 Selects an appropriately tailored set of baseline security controls

Yes

Section 5: Risk Management

5.1.7 Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation

Yes

5.1.8 Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system

No

Comments: The security controls were assessed for only 34 of OPM's 47 major applications in FY 2012.

5.1.9 Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable

Yes

5.1.10 Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials

No

Comments: OPM's continuous monitoring program is not fully implemented (see comments in section 1).

5.1.11 Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization.

Yes

5.1.12 Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO).

Yes

5.1.13 Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks

Yes

Section 5: Risk Management

5.1.14 Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies. (SP 800-18, SP 800-37)

Yes

5.1.15 Security authorization package contains Accreditation boundaries for Organization information systems defined in accordance with government policies.

Yes

5.2 Please provide any additional information on the effectiveness of the Organization's Risk Management Program that was not noted in the questions above.

Risk Management

Section 6: Security Training

6.1 Has the Organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

6.1.1 Documented policies and procedures for security awareness training (NIST 800-53: AT-1)

Yes

6.1.2 Documented policies and procedures for specialized training for users with significant information security responsibilities

Yes

6.1.3 Security training content based on the organization and roles, as specified in Organization policy or standards

Yes

6.1.4 Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other Organization users) with access privileges that require security awareness training

Yes

6.1.5 Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other Organization users) with significant information security responsibilities that require specialized training

Yes

Section 6: Security Training

6.1.6 Training material for security awareness training contains appropriate content for the Organization (SP 800-50, SP 800-53).

Yes

6.2 Please provide any additional information on the effectiveness of the Organization's Security Training Program that was not noted in the questions above.

Security Training

Comments:

OPM employees with significant information security responsibilities are required to take specialized security training in addition to the annual awareness training. However, only 86% of employees identified as having information security responsibility completed the required specialized security training in FY 2012.

Section 7: Plan Of Action & Milestones (POA&M)

7.1 Has the Organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

7.1.1 Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation

Yes

7.1.2 Tracks, prioritizes and remediates weaknesses

Yes

7.1.3 Ensures remediation plans are effective for correcting weaknesses

No

Comments:

See comment in 7.1.4

7.1.4 Establishes and adheres to milestone remediation dates

No

Comments:

Our review of 2012 POA&Ms indicated that many system owners are not meeting the self-imposed remediation deadlines listed on the POA&Ms. Twenty-two of OPM's 47 systems have POA&M items that are greater than 120 days overdue. We believe that this indicates that POA&M remediation plans are not effective for correcting weaknesses.

Section 7: Plan Of Action & Milestones (POA&M)

7.1.5 Ensures resources are provided for correcting weaknesses

No

Comments:

We interviewed the system owners of 10 OPM systems with overdue POA&M items. Each owner stated that although they have identified the resources required to address the POA&M items, these resources are not currently available.

7.1.6 POA&Ms include security weaknesses discovered during assessments of security controls and requiring remediation. (Do not need to include security weakness due to a Risk Based Decision to not implement a security control) (OMB M-04-25)

Yes

7.1.7 Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25)

No

Comments:

Our review indicated that 11 POA&Ms have not identified the resources that would be required to address POA&M weaknesses, as required by OPM's POA&M policy.

7.1.8 Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25)

Yes

7.2 Please provide any additional information on the effectiveness of the Organization's POA&M Program that was not noted in the questions above.

POA&M

Section 8: Remote Access Management

8.1 Has the Organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

8.1.1 Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST 800-53: AC-1, AC-17)

Yes

Section 8: Remote Access Management

- 8.1.2 Protects against unauthorized connections or subversion of authorized connections.
Yes
- 8.1.3 Users are uniquely identified and authenticated for all access (NIST 800-46, Section 4.2, Section 5.1)
Yes
- 8.1.4 Telecommuting policy is fully developed (NIST 800-46, Section 5.1)
Yes
- 8.1.5 If applicable, multi-factor authentication is required for remote access (NIST 800-46, Section 2.2, Section 3.3)
Yes
- 8.1.6 Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms
Yes
- 8.1.7 Defines and implements encryption requirements for information transmitted across public networks
Yes
- 8.1.8 Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication are required
No

Comments: Remote connections via VPN do not timeout after 30 minutes of inactivity.

- 8.1.9 Lost or stolen devices are disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines)
Yes
- 8.1.10 Remote access rules of behavior are adequate in accordance with government policies (NIST 800-53, PL-4)
Yes
- 8.1.11 Remote access user agreements are adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6)
Yes
- 8.2 Please provide any additional information on the effectiveness of the Organization's Remote Access Management that was not noted in the questions above.
Remote Access Management

Section 9: Contingency Planning

Section 9: Contingency Planning

- 9.1 **Has the Organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:**

No

Comments:

It has been over 4 years since OPM has tested the contingency plans of all of its major information systems within one fiscal year (see 9.1.4). In addition, one of OPM's major general support systems is not subject to adequate disaster recovery testing (see 9.1.7). We believe that this indicates that OPM does not have a FISMA-compliant enterprise-wide business continuity / disaster recovery program.

- 9.1.1 **Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST 800-53: CP-1)**

Yes

- 9.1.2 **The Organization has performed an overall Business Impact Analysis (BIA) (NIST SP 800-34)**

Yes

- 9.1.3 **Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures (NIST SP 800-34)**

Yes

- 9.1.4 **Testing of system specific contingency plans**

No

Comments:

OPM's Information Security Privacy and Policy Handbook requires that the contingency plan for each information system be tested at least annually using information system specific tests and exercises. However, we received evidence that contingency plans were tested for only 39 of 47 systems in FY 2012. Of the contingency plan tests we did receive, we continue to notice inconsistency in the quality of the documentation produced for various OPM systems. Our reviews have indicated that the decentralized program office personnel currently responsible for conducting the contingency plan tests do not have the technical experience to adequately perform the task. We expect that OPM's planned centralized security function will improve this weakness, as contingency plan tests will be performed by the security professionals that report to the CIO.

Section 9: Contingency Planning

9.1.5 The documented business continuity and disaster recovery plans are in place and can be implemented when necessary (FCD1, NIST SP 800-34)

Yes

9.1.6 Development and fully implementable of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST 800-53)

Yes

9.1.7 Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans

No

Comments:

Many OPM systems reside on one of the agency's general support systems. The OCIO conducts a full recovery test of the Enterprise Server Infrastructure general support system (i.e., the mainframe and associated systems) on an annual basis. However, the LAN/WAN general support system is not subject to a full functional disaster recovery test on a routine basis. In the FY 2011 FISMA audit report we recommended that the OCIO implement a centralized (agency-wide) approach to contingency plan testing. We were informed that a single synchronized functional test is not feasible due to logistical and resource limitations. However, the intent of the recommendation is to ensure that all elements of the general support systems are subject to a full functional disaster recovery test each year. This recommendation can be remediated if each general support system is subject to a full functional test each year, even if it must be broken into a series of smaller tests.

9.1.8 After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34)

No

Comments:

As mentioned in 9.1.4, only 39 out of OPM's 47 major applications were subject to a contingency plan test. Of those that were performed, the after action reports lacked quality and consistency.

9.1.9 Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53)

Yes

9.1.10 Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53)

Yes

9.1.11 Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53)

Yes

Section 9: Contingency Planning

9.1.12 Contingency planning that consider supply chain threats

Yes

9.2 Please provide any additional information on the effectiveness of the Organization's Contingency Planning Program that was not noted in the questions above.

Contingency Planning

Section 10: Contractor Systems

10.1 Has the Organization established a program to oversee systems operated on its behalf by contractors or other entities, including Organization systems and services residing in the cloud external to the Organization? Besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes:

No

Comments:

We do not believe that OPM has a program in place to adequately oversee systems operated by a contractor (see 10.1.2).

10.1.1 Documented policies and procedures for information security oversight of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud

Yes

10.1.2 The Organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and Organization guidelines

No

Comments:

OPM's OCIO distributes an annual Site Survey Assessment that program offices are required to complete for all contractor operated systems. The survey requires the program office to document the physical, operational, organizational, and technical security controls in place at the contractor facilities. Although the Site Survey Assessment is conceptually a good approach to overseeing contractor systems, the contractor is permitted to complete the survey themselves as opposed to an OPM employee or independent third party. We do not believe that this constitutes adequate independent oversight. In our opinion, adequate oversight over contractor systems would require a federal employee or an independent third party to conduct the annual security controls tests as well as the triennial system Authorization.

Section 10: Contractor Systems

10.1.3 A complete inventory of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud

No

Comments:

OPM's system inventory adequately includes systems run by contractors. However, it does not indicate which systems operate in a cloud environment.

10.1.4 The inventory identifies interfaces between these systems and Organization-operated systems (NIST 800-53: PM-5)

Yes

10.1.5 The Organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates

Yes

10.1.6 The inventory of contractor systems is updated at least annually.

Yes

10.1.7 Systems that are owned or operated by contractors or entities, including Organization systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines

Yes

10.2 Please provide any additional information on the effectiveness of the Organization's Contractor Systems Program that was not noted in the questions above.

Contractor Systems

Section 11: Security Capital Planning

11.1 Has the Organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

Comments:

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.

Section 11: Security Capital Planning

11.1.1 Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process

Yes

11.1.2 Includes information security requirements as part of the capital planning and investment process

Yes

11.1.3 Establishes a discrete line item for information security in organizational programming and documentation (NIST 800-53: SA-2)

Yes

11.1.4 Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST 800-53: PM-3)

Yes

11.1.5 Ensures that information security resources are available for expenditure as planned

Yes

11.2 Please provide any additional information on the effectiveness of the Organization's Security Capital Planning Program that was not noted in the questions above.

Security Capital Planning