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 2010

Report No. 4A-CI-00-10-019

Date: November 10, 2010

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT
FY 2010

WASHINGTON, D.C.

Report No. **4A-CI-00-10-019**

Date: 11/10/10

Michael R. Esser
Assistant Inspector General
for Audits

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT
FY 2010

WASHINGTON, D.C.

Report No. **4A-CI-00-10-019**

Date: 11/10/10

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 Inspector General (OIG) has significant ongoing concerns regarding the overall quality of the information security program at OPM.

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

Although we acknowledge that some limited progress was made in FY 2010 to improve OPM's security program, we continue to consider the IT security management structure, insufficient

staff, and the lack of policies and procedures to be a material weakness in OPM's IT security program.

In addition, we are adding a second material weakness related to the management of OPM's Certification and Accreditation (C&A) process. The C&A concerns were reported as a significant deficiency in the FY 2008 and FY 2009 Federal Information Security Management Act (FISMA) audit reports. Specifically, we noted that not all systems at OPM have an active C&A, there is a wide range of quality in the C&A packages from various program offices, and the Office of the Chief Information Officer (OCIO) does not have the resources to facilitate the C&A process.

The agency has recently appointed a new Senior Agency Information Security Official. However, it remains to be seen whether it will commit the necessary resources and develop the appropriate functions required of this role. We will reevaluate this issue during the FY 2011 FISMA audit.

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

- The OIG does not agree with the number of systems identified in OPM's master system inventory. The OCIO takes a passive approach to maintaining the inventory, increasing the risk that applications containing sensitive data are operating in a production environment without being subject to the IT security controls required by FISMA.
- The OCIO does not maintain a single centralized inventory of the computer hardware in its data centers.
- The OCIO has developed a Windows XP image that is generally compliant with Federal Desktop Core Configuration standards. However, this image has not been implemented on any production workstations.
- The OCIO has developed thorough incident response and reporting capabilities.
- The OCIO has implemented a process to provide annual IT security and privacy awareness training to all OPM employees and contractors. However, controls related to providing specialized security training to individuals with information security responsibility could be improved.
- A Plan of Action and Milestones (POA&Ms) should be continuously managed for all agency systems, but we found that POA&Ms were updated every quarter in FY 2010 for only 35 of OPM's 43 systems.
- All 30 of the recommendations from the FY 2009 FISMA audit were appropriately incorporated into the OCIO POA&M. However, POA&M items from the system-specific audits conducted by the OIG do not appear in the POA&M of the individual systems.
- The POA&Ms for 9 OPM systems contain security weaknesses with remediation activities over 120 days overdue.
- [redacted]

- [redacted]
- The OCIO has not developed a formal strategy to identify and continuously monitor the high-risk security controls for OPM information systems.
- The OCIO does not currently maintain a published list of common security controls.
- The OCIO and other OPM program offices maintain up-to-date contingency plans for only 36 of the 43 systems on OPM's master system inventory. The contingency plans for only 30 of 43 systems were adequately tested in FY 2010.
- OPM does not have a formal policy providing the OCIO and other program offices guidance on the appropriate oversight of contractors and contractor-run systems. In addition, the security controls were not tested in FY 2010 for 7 of 11 contractor-operated systems.

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. System Inventory 7
III. Certification and Accreditation Program 9
IV. Security Configuration Management 15
V. Incident Response and Reporting Program 18
VI. Security Training Program 18
VII. Plan of Action and Milestones Program 20
VIII. Remote Access Program 24
IX. Account and Identity Management Program 26
X. Continuous Monitoring Program 26
XI. Contingency Planning Program 28
XII. Program to Oversee Contractor Systems 30
XIII. Follow-up From Prior OIG Audit Recommendations 31
Major Contributors to this Report 43

Appendix I: Status of Prior Audit Recommendations Issued by the Office of the Inspector General

Appendix II: Office of Chief Information Officer's October 7, 2010 response to the draft audit report, issued September 22, 2010.

Appendix III: Fiscal Year 2010 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 evaluation of OPM's security program and practices. As part of our evaluation, we reviewed OPM's FISMA compliance strategy and documented the status of its compliance efforts.

Background

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

FISMA reemphasizes the Chief Information Officer's 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, OMB issued memorandum M-10-15, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. This memorandum provides a consistent form and format for agencies to report to OMB. It identifies a series of reporting topics that relate to specific agency responsibilities outlined in FISMA. Our audit and reporting strategies were designed in accordance with the above OMB guidance.

Objectives

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

- System Inventory;
- Status of Certification and Accreditation Program (C&A);
- Status of Security Configuration Management;
- Status of Incident Response and Reporting Program;
- Status of Security Training Program;
- Status of Plans of Actions and Milestones (POA&M) Program;
- Status of Remote Access Program;
- Status of Account and Identity Management Program;
- Status of Continuous Monitoring Program;

- Status of Contingency Planning Program; and
- Status of Agency Program to Oversee Contractor Systems.

In addition, we evaluated the security controls of two 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 2010.

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

- Benefits Financial Management System (OIG Report No. 4A-CF-00-10-018)
- Annuity Roll System (OIG Report No. 4A-CF-00-10-047)

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.

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

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:

- OPM Information Technology Security Policy Volumes 1 and 2;
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- OMB Memorandum M-10-15, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management;
- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information;
- OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- National Institute for Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security;
- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems;
- NIST SP 800-53 Revision 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 2010 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 the OIG's FY 2010 FISMA audit of OPM's IT Security Program. Several recommendations issued in FY 2010 were rolled-forward from prior OIG audit reports, including:

- Report 4A-CI-00-09-053: "Flash Audit Alert – Information Technology Security Program at the U.S. Office of Personnel Management"
- Report 4A-CI-00-07-015: "Audit of the Privacy Program at OPM – FY 2007"
- Report 4A-CI-00-06-016: "Federal Information Security Management Act Audit – FY 2006"
- Report 4A-CI-00-07-007: "Federal Information Security Management Act Audit – FY 2007"
- Report 4A-CI-00-08-022: "Federal Information Security Management Act Audit – FY 2008"
- Report 4A-CI-00-09-031: "Federal Information Security Management Act Audit – FY 2009"

I. Information Security Governance

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

a) IT Security Policies and Procedures

OPM's failure to adequately update its IT security and privacy policies and procedures has been highlighted in the past four OIG FISMA audit reports, and has been identified as a material weakness in the IT security program in the FY 2007, FY 2008, and FY 2009 reports.

The absence or severely outdated nature of the following policies, procedures, or guidance has directly led to OIG audit findings in FY 2009 and 2010 (*this is not intended to be a comprehensive list of missing policies at OPM*):

- Guidance for developing contingency plans, procedures for routinely conducting contingency plan tests, and templates for reporting test results;
- [redacted]
- Guidance for developing risk assessments;
- Guidance for developing information system security plans;
- Policy and procedures related to oversight of systems operated by a contractor;
- Policy related to roles and responsibilities for the Independent Verification and Validation (IV&V) process and procedures for managing an IV&V;
- Guidance for establishing agreements for interfacing systems;

- [redacted]
- Policy on remote access and telecommuting; and
- Policy on patch management.

Although several new security and privacy documents were published in FY 2010, this area continues to be a major concern as the limited IT policies available do not provide OPM employees with adequate guidance to secure the agency's information systems.

Recommendation 1 ***(Roll-Forward from OIG Reports 4A-CI-00-09-031 Recommendation 30, 4A-CI-00-09-053 Recommendation 2, 4A-CI-00-08-022 Recommendation 19, 4A-CI-00-07-007 Recommendation 3 and 9, 4A-CI-00-07-015 Recommendation 1, and 4A-CI-00-06-016 Recommendation 6)***

We recommend that the OCIO develop up-to-date and comprehensive IT security policies and procedures, and publish these documents to THEO, and a plan for updating them at least annually.

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation of the status of the IT security policies and procedures. The IT security and privacy policy volumes 1 and volume 2 were last updated and posted on THEO in August 2009. The CIO understands that additional policy updates are required to comply with guidance issued by NIST during the last year and to address some deficiencies in the current policies. The Bureau of the Public Debt (BPD) has been retained through an Interagency Agreement to update and to bring IT Security and Privacy policies into OPM and FISMA compliance. A kickoff meeting was held for this project on September 2010 and BPD is expected to be on site to collect policy requirements during the next 60 days. A comprehensive IT security and Privacy handbook is expected to be completed in FY2011.

This recommendation also cited the need for procedures and a number of procedures were created or updated and posted on THEO in 2009/2010 including:

- ***Certification and Accreditation Guide (July 2009)***
- ***Incident Response and Reporting Guide (July 2009)***
- ***LAN Complex Passwords (June 2009)***
- ***OPM Computer User Responsibilities (June 2009)***
- ***Plan of Action and Milestone (POA&M Standard Operating Procedure (September 2009)***
- ***Process for Analyzing New and Emerging Information Security and Privacy Requirements (July 2009)***
- ***System Access Authorization Procedure (July 2009)***
- ***Privacy Impact Assessment (PIA) Guide (April 2010)***
- ***System of Records Notice (SORN) Guide (April 2010)***

The CIO believes that the above procedures have enhanced IT security and privacy at OPM and understands that additional work needs to be done to develop new procedures and to enhance existing ones as necessary. Current procedures will be revisited and additional ones will be developed in FY2011 as necessary."

OIG Reply:

The majority of the new procedures referenced in the OCIO response were issued during FY 2009. Although this limited progress was acknowledged in the FY 2009 OIG FISMA audit report, we continued to label this issue as a material weakness in OPM's IT security program. The addition of a PIA Guide and SORN Guide in FY 2010 again represents very limited progress in improving OPM's IT security and privacy policies, and this issue continues to represent a material weakness in FY 2010.

b) Information Security Management Structure

In FY 2009, the OIG issued a Flash Audit Alert to OPM's Director highlighting our concerns with the agency's IT security program. We also expanded the existing IT security policy material weakness to include concerns with the agency's overall information security governance and the information security management structure in the OCIO.

At the end of FY 2009, OPM had operated without a permanent Senior Agency Information Security Officer (SAISO) for over 18 months. Although a new SAISO was appointed in FY 2010, 24 of the 30 audit recommendations issued in the FY 2009 FISMA audit report, and 2 of the 4 recommendations issued in the Flash Audit Alert, have been rolled-forward into this FY 2010 FISMA report. We believe this indicates that the OCIO does not have adequate resources to effectively remediate weaknesses in OPM's IT security program.

Recommendation 2 ***(Roll-forward from OIG Report 4A-CI-00-09-053 Recommendation 3)***

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation of the staffing situation in the IT Security and Privacy Group. During the past five months, a Senior Agency Information Security Officer has being hired and the staff complement in the security and privacy group has increased from [redacted] FTEs along with contractor resources as needed. Recognizing that additional staff resources are needed, the CIO believes that incremental progress is being made in this area."

OIG Reply:

Although the OCIO has been authorized to hire [redacted] full time employees, only [redacted] of these positions have been filled to date. We continue to believe that the OCIO does not have adequate resources to effectively remediate weaknesses in OPM's IT security program, and we recommend that the IT Security and Privacy Group increase its staffing resources.

In September 2010, the OCIO informed the OIG that OPM has secured funding to enter into an interagency agreement with the Bureau of Public Debt for assistance in developing a comprehensive IT security handbook. The SAISO is also actively recruiting to fill several open positions in the OCIO.

Although the OIG acknowledges that OPM appears to be taking steps to improve its security program, we continue to consider the insufficient resources and security governance in the OCIO and the lack of policies and procedures to be a material weakness in OPM's IT security program.

II. System Inventory

OPM has identified 43 major systems within 8 of its program offices. OPM's system inventory indicated that these 43 systems were comprised of the following security categorizations (as defined by Federal Information Processing Standards Publication 199): 7 high, 34 moderate, and 2 low. The inventory also indicated that 32 systems are operated by OPM within its own IT infrastructure and 11 are operated by a contractor facility on behalf of the agency.

The OIG does not agree with the number of systems identified in OPM's master inventory. In FY 2010, the following anomalies were detected with the agency's inventory:

- An OIG audit of one system in FY 2010 revealed that several applications were inappropriately bundled into that single system on the inventory. The OIG recommended that this system be divided into at least four separate applications on the inventory.
- An OIG audit of a second system containing multiple applications revealed that the program office owning the system does not have a clear understanding of which specific applications are actually part of that system. Several applications were removed from this system and may not be accounted for elsewhere on the inventory.
- One system has been in production for many years but was not added to the inventory and subjected to a C&A until FY 2010.
- The OIG received copies of POA&Ms for three systems that did not appear on the inventory.

OPM's OCIO is responsible for maintaining the agency's master system inventory. The OCIO relies heavily on OPM's program offices to inform them of updates to the system inventory (e.g., new or decommissioned systems). Although monthly email reminders are sent to the Designated Security Officer (DSO) community asking for inventory updates, the

OCIO generally maintained a passive approach to maintaining the agency's system inventory in FY 2010.

In September 2010, the OCIO began the process of surveying OPM's program offices in an attempt to identify any systems not currently reported on the inventory. The OIG believes that this is a good step toward implementing an active strategy for maintaining the system inventory. However, the OCIO needs to implement additional techniques to help ensure that the system inventory identifies all major applications in OPM's operating environment. Such techniques could include, but are not limited to:

- Routine review of database and hardware inventories to search for applications not accounted for on the system inventory;
- Use of software tools to scan the network environment for rogue hardware devices that are not accounted for on the system inventory; and
- Periodic survey of OPM employees (not just the DSO community) to inquire about applications used in their job function.

Failure to properly maintain OPM's master system inventory increases the risk that applications containing sensitive data are running in a production environment without being subject to the IT security controls required by FISMA. We consider the weaknesses related to the management of the system inventory to be a significant deficiency in OPM's information technology security program.

Recommendation 3

We recommend that the OCIO develop and implement an active strategy to maintain up-to-date information regarding OPM's master system inventory.

OCIO Response:

"The CIO concurs with this recommendation and has already taken steps through the issuance of a data call to the IT Security Working Group on September 8, 2010 to identify systems used by OPM that are not on the FISMA system inventory. The CIO has also initiated an internal review to determine if applications were inappropriately bundled into other larger systems as previously reported in prior audit findings. Additional systems identified from the data call and internal system review will be evaluated for addition to the master system inventory."

OIG Reply:

We acknowledge the limited progress the OCIO has made in improving the quality of its system inventory. However, the data call referenced in the OCIO response relies on other OPM program offices to notify the OCIO of new or modified information systems. We continue to recommend that the OCIO develop and implement an active strategy to maintain the system inventory using some or all of the suggested techniques outlined above.

III. Certification and Accreditation Program

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. Each major application at OPM is subject to the C&A process every three years.

The OIG's FY 2008 and FY 2009 FISMA audit reports stated that weaknesses in OPM's C&A process were a significant deficiency in the internal control structure of the agency's IT security program. The weaknesses cited related to inadequate management of the process and incomplete, inconsistent, and poor quality C&A products. In FY 2010 these longstanding conditions not only continued, but actually degraded. As a result, we are now reporting a material weakness in the IT security control structure related to OPM's C&A process.

We believe that the root causes of these issues include insufficient staffing in the IT Security and Privacy Group, a lack of policy and procedures, and the decentralized DSO model in place at OPM.

Insufficient staffing and the lack of documented policies are discussed in the Security Governance section of this report (section I). The third underlying weakness, in our opinion, relates to how OPM staffs the DSO position. OPM chose to implement a decentralized model in which the DSOs are typically appointed by and report to the program offices that own major computer systems. Very few of the DSOs have any background in information security, and most are only managing their security responsibilities as a collateral duty to their primary job function.

Perhaps in recognizing the inherent weaknesses in this arrangement, the OCIO established an Information Technology Security Working Group to provide guidance to the DSO community in a series of monthly meetings. Initially these meetings were a useful forum that involved training in IT security, discussion of various security-related topics, and the dissemination of emerging guidance. However, the meetings eventually degenerated into sessions where DSOs were upbraided for not meeting the required FISMA metrics; the focus seemed to be on "playing the FISMA numbers game" rather than implementing the foundations of a successful IT security program. Of late the DSOs are complaining about being overly burdened as the OCIO, with limited resources, asks more of the DSO community.

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

Recommendation 4

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

OCIO Response:

"The CIO concurs with this recommendation. The overall IT security governance at OPM can be improved by implementing a centralized information security governance structure consisting of IT security professionals."

The sections below provide a detailed evaluation of OPM's C&A program.

a) C&A policy

In July 2009, the OCIO published an agency-wide Certification and Accreditation Guide. The C&A Guide addresses the roles and responsibilities of key personnel, a walkthrough of the C&A process, and a listing of the various security documents that are required elements of a C&A, including:

- System Categorization;
- Privacy Impact Assessment (PIA);
- Information System Security Plan (ISSP);
- Risk Assessment;
- Security Control Test and Evaluation Plan and Report;
- Contingency Plan;
- System of Records Notice; and
- Plans of Action and Milestones.

However, OPM's C&A Guide does not provide standard forms, templates, or detailed guidance on how to prepare each of the required elements. The lack of such guidance has led to extreme inconsistencies in the quality of C&A packages for various OPM systems (see "Quality and Consistency of C&A Packages" below).

b) Appropriate use of the C&A process

As referenced in Section II above, the OIG identified one OPM system that was in production for several years without being subject to a C&A.

In addition, the prior C&A for six additional systems from OPM's inventory expired in FY 2010, and a new C&A has not been completed. Although an "Interim Authorization to Operate" (IATO) was issued for these systems, they are currently running in a production environment without an active C&A.

An IATO may be appropriate to use in special circumstances where legitimate business reasons result in a C&A package not being completed before the prior C&A expires. However, we believe this process is abused at OPM and is used to extend the authorization to operate for program offices that did not adequately plan for their systems' required C&A.

Recommendation 5 ***(Roll-Forward from OIG Reports 4A-CI-00-09-031 Recommendation 16 and 4A-CI-00-08-22 Recommendation 9)***

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. Program offices are responsible for the security and C&A of their systems. C&As are often contracted to various entities that employ different styles in preparing the final packages and this explains why all C&A packages do not look alike. The CIO believes that all completed C&A packages must properly address required security controls and contain required artifacts per the OPM C&A Guide, and that the look and feel of packages is a reflection of the various sources contracted by the program offices to complete the packages.

Regarding, the six systems with expired C&A, the CIO agrees that all production systems should have a current C&A. However, the OPM procurement process can be lengthy depending on workload has an effect on getting contracts and interagency agreements for C&A in place. The extended Authority to Operate for the six systems was issued in support of OPM mission support activities."

OIG Reply:

FISMA states that it is the responsibility of the OCIO to maintain an agency-wide information security program. Although the C&A process is a shared effort with OPM program offices, the OCIO has the primary responsibility to ensure that all C&A packages are completed in a timely manner and are of consistent quality.

The OIG is discouraged to see that the OCIO references the lengthy OPM procurement process as justification for having production systems operating without a C&A. The requirement for federal information systems to have an active C&A has been in place since 2003, and there has been ample time to properly budget IT security into the system development lifecycle. We believe that poor planning, insufficient staffing resources, and the OCIO's lack of authority over DSOs all contribute to this material weakness.

We believe that the centralized C&A approach referenced in Recommendation 4 would allow the OCIO to more efficiently manage the C&A process and ensure that an active C&A exists for each OPM system as required by FISMA.

c) Quality and consistency of C&A packages

The OIG reviewed the full C&A packages of 15 systems that were subject to a C&A during FY 2010. Although the packages we reviewed contained all of the elements required by OPM's C&A Guide, the quality of these packages varied significantly between systems.

The development of a C&A package is the responsibility of the OPM program office that owns the system. Each program office assigns a DSO to manage the security of its systems. The decentralized nature of the DSO community means that individuals with varying skill sets are tasked with C&A related responsibilities often as a collateral duty in addition to their normal job function.

Although various forms of general guidance are available to assist program offices in the development of C&A elements, the OCIO has not implemented centralized policies, guidelines, or templates outlining how various C&A elements should be completed for OPM systems. As a result, the content and quality of a specific C&A element vary widely between systems. During our review of FY 2010 C&A packages, we noticed the highest quality variance between the security controls tests (see "Testing of Security Controls," below), contingency plans (see section XI), risk assessments, and ISSPs of these systems.

Recommendation 6

We recommend that the OCIO develop a risk assessment policy to provide guidance to program offices conducting a risk assessment as part of the C&A process.

OCIO Response:

"The CIO does not concur with this recommendation. Risk assessment policies are documented in the current IT security and Privacy policy volume 2 that is posted on THEO. However, risk assessment policy will be revisited and updated in the new IT Security policy updates that BPD has been retained to complete."

OIG Reply:

The IT Security and Privacy Policy Volume 2 states that the OCIO must develop a risk assessment policy along with procedures for facilitating the implementation of the policy. However, no such policies and procedures are contained within the document. The extreme range in quality between risk assessments conducted by various OPM program offices indicates that the OCIO has not provided adequate risk assessment guidance. We continue to recommend that the OCIO develop a risk assessment policy to provide guidance to program offices conducting a risk assessment as part of the C&A process.

Recommendation 7

We recommend that the OCIO develop an ISSP policy to provide guidance to program offices developing a security plan as part of the C&A process.

OCIO Response:

"The CIO does not concur with this recommendation. Information Systems Security Plan policies are documented in the current IT security and Privacy policy volume 2 that is posted on THEO. The policies also references NIST security plan templates that can be used to build a security plan. However, IT security plans policy will be updated to provide additional as part of the BPD policy update project.

Regarding the review of C&A packages, two full time resources have been hired to review C&A packages and to provide guidance to the DSO community. One of these resources is already onboard and the second is expected to start work after completing the necessary new employee onboarding procedures."

OIG Reply:

The IT Security and Privacy Policy Volume 2 states that system owners must work with the OCIO and DSOs to develop information system security plans. However, the policy provides no actual guidance for doing so. We continue to recommend that the OCIO develop an ISSP policy to provide guidance to program offices developing a security plan as part of the C&A process.

d) OCIO management of C&A process

The OCIO is responsible for assisting program offices in the development of C&A packages for their systems. OPM's C&A Guide also states that the OCIO must review completed C&A packages for quality and completeness before recommending the system for accreditation.

Although the OCIO has procedures for conducting post-completion reviews of C&A packages, the post-completion review for at least one system (the LAN/WAN infrastructure) was conducted after the certification and accreditation statements were signed. The reviewer of the LAN/WAN C&A package found several errors and weaknesses in the documentation and made recommendations for improvement, but these were not presented to the certification and accreditation authority prior to the signing of the C&A statements.

In addition, the OCIO does not have the resources available to actively participate in the planning or development of the C&A packages for each agency system. Inadequate oversight of the C&A process from the OCIO has led to OPM program offices developing inconsistent and low quality C&A packages.

Recommendation 8

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO has doubled the number of full time resources assigned to the C&A program and this increase in resources will improve the quality of C&A packages. C&A packages found to be of poor quality are being returned to for rework for correction of deficiencies."

e) Testing of security controls

Although a full C&A is required for each system every three years, the security controls of that system must be tested on an annual basis. An annual test of security controls provides a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. Failure to complete a security controls test increases the risk that agency officials are unable to make informed judgments to appropriately mitigate risks to an acceptable level.

We conducted a review of the documentation resulting from the security controls tests for each of the 43 systems in OPM's inventory. Our evaluation indicated that the IT security controls had been adequately tested for only 28 of OPM's 43 systems during FY 2010.

There was a wide range of quality amongst the 28 security control tests that were conducted. Some program offices tested all security controls applicable to that system while others tested only a small subset. There was also a variance in the security controls that program offices assumed to be "common controls" inherited from OPM's IT and facility infrastructures (see section X, Continuous Monitoring). In addition, the tests were documented in many different formats and templates. We believe that these inconsistencies are a result of OPM's lack of agency-wide policy or guidance on how to adequately test information system security controls.

Recommendation 9 ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 5)***

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The Information Security and Privacy Policy Volume 1 requires security controls to be Periodically assessed and CIO security staff works with the DSO community on annual testing efforts including keeping track of the number of systems that have tested their security controls. We will enhance the current security policy in the security handbook that is under development and provide additional guidance to DSOs to enhance the testing of security controls."

OIG Reply:

The IT Security and Privacy Policy Volume 1 states that information system security controls must be assessed on a periodic basis, but provides no guidance for doing so. The extreme range in quality between security control tests conducted by various OPM program offices indicates that the OCIO has not provided adequate guidance on this topic. We continue to recommend that the OCIO develop a policy for adequately testing the security controls of OPM's systems, and provide training to the DSO community related to proper security control testing.

Recommendation 10 ***(Roll-Forward from OIG Reports 4A-CI-00-09-031 Recommendation 6 and 4A-CI-00-08-022 Recommendation 1)***

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO staff continues works with the DSO community to ensure that security controls have been tested for all systems. The CIO security staff sends out a reminder to all DSOs each month informing them to complete required security controls testing and assist with technical guidance. We will continue to work with the DSO community and escalate systems where security controls have not been tested to the associated director in the specific business area."

IV. Security Configuration Management

The sections below detail the controls OPM has in place regarding the technical configuration management of its major applications and user workstations.

a) Agency-wide security configuration policy

The OCIO has implemented an agency-wide Configuration Management Policy. This policy was updated during FY 2010 and outlines the process for maintaining a securely configured network environment.

The OCIO has also implemented a patch management policy that outlines the responsibilities and procedures for ensuring that OPM servers are routinely patched. However, this policy has not been updated since August 2005. In August 2010, the OCIO informed the OIG that this policy is in the process of being updated.

Recommendation 11 ***(Roll-Forward from OIG Report No. 4A-CI-00-09-031 Recommendation 25)***

We recommend that the OCIO develop and publish to THEO an up-to-date Patch Management Policy.

OCIO Response:

"The CIO does not concur with this recommendation. The OPM ISPP details the high level patch (flaw remediation) requirements and agency policy. (See ISPP Volume 2, page 71. 800-53 rev 3 Control SI-2). Low level procedures exist and are utilized by the Network Management administrators to patch desktops and servers. Ongoing improvements to the patch management process are being tested and implemented as new tools and processes become available. Current initiatives include procurement requests for enterprise-wide patch and vulnerability management tools (Big Fix and Window SUS) scheduled for implementation in FY 2011."

OIG Reply:

The Information Security and Privacy Policy Volume 2 simply states that system stakeholders must "identify, report, and correct flaws discovered in the information system software or hardware." This does not constitute a comprehensive patch management policy. We acknowledge that low level patch management procedures exist, but they have not been updated in over five years. We continue to recommend that the OCIO develop and publish to THEO an up-to-date Patch Management Policy.

b) Management of hardware inventory

OPM currently uses several Excel spreadsheets to track its computer hardware inventory. These spreadsheets are manually updated when new hardware is purchased or old hardware is decommissioned. Separate spreadsheets are maintained by different individuals for Windows severs, Linux servers, and all servers operated by OPM's Federal Investigative Services program office. However, each of these spreadsheets is maintained independently from the other inventories, and no individual at OPM maintains a single inventory listing that contains all computer hardware owned by the agency. Therefore, the OCIO is unable to attest that all computer hardware in OPM's operating environment is accounted for.

Recommendation 12

We recommend that the OCIO develop a single centralized agency-wide hardware inventory.

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. Network Management is actively implementing a centralized agency-wide automated hardware inventory tracking system. Asset tags are being applied to all accountable IT assets and pending procurements for scanning equipment are expected to quickly bring the outstanding inventory under control. Daily and weekly automated inventory reports are now being produced and internal audits of the process will begin this quarter."

Recommendation 13

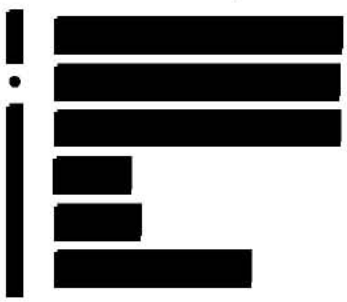
We recommend that the OCIO develop and implement a strategy for using automated techniques for tracking hardware inventory.

OCIO Response:

"The CIO concurs with this recommendation."

c) Standard baseline configurations

OPM maintains standard baseline configurations and/or build sheets for all operating platforms reviewed by the OIG, including:



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

d) Federal Desktop Core Configuration

OPM has developed a Windows XP standard image that is generally compliant with Federal Desktop Core Configuration (FDCC) standards and has documented nine deviations between this image and FDCC requirements.

As of September 30, 2010, OPM's FDCC compliant image has not been rolled out to the majority of OPM workstations.

Recommendation 14 ***(Roll-Forward from OIG Reports 4A-CI-00-09-031 Recommendation 26 and 4A-CI-00-08-022 Recommendation 16)***

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

OCIO Response:

"The CIO concurs with this recommendation and offers the following clarifying remarks: An FDCC workstation baseline image has been created and is currently being deployed. All new workstations and all agency laptops are currently secured utilizing an FDCC (USGBC) compliant image. The FDCC image has been rolled out to 1200 laptops and 800 desktops as of this date. Image deployment and enforcement

of the legacy workstations is currently an active project and is being pushed through domain GPO. The addition of workstations occurs daily and is scheduled to have full completion by the end of the first quarter of FY 2011. Part of the delay in implementation was due to working with the union to assess the impact on employees."

V. Incident Response and Reporting Program

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

a) Identifying and reporting incidents internally

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

b) Reporting incidents to US-CERT

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

c) Reporting incidents to law enforcement

The Incident Response and Reporting policy states that security incidents should also be reported to law enforcement authorities, where appropriate. OPM notifies OIG law enforcement of security incidents with a monthly report outlining all incidents where sensitive data was lost.

VI. Security Training Program

The following sections detail OPM's methodology for providing security awareness training to all employees and specialized security training to individuals with IT security responsibility.

a) Security awareness training

The OCIO has implemented a process to provide annual IT security and privacy awareness training to all OPM employees and contractors. The training is conducted through an interactive web-based course. The course introduces employees and contractors to the basic concepts of IT security and privacy, including topics such as the importance of information security, security threats and vulnerabilities, viruses and malicious code, privacy training, peer-to-peer software, and the roles and responsibilities of users.

Over 99 percent of OPM's employees and contractors completed the security awareness training course in FY 2010.

b) Specialized security training

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

The OCIO has developed a table outlining the security training requirements for specific job roles. The OCIO uses a spreadsheet to track the security training taken by employees that have been identified as having security responsibility. Of those identified, 87 percent have completed at least one hour of specialized security training in FY 2010. However, a significant portion (33 percent) of the individuals on the spreadsheet are listed with a job role that does not appear on the training requirements table (i.e., "significant responsibility"), making it impossible to determine whether these individuals received adequate training in FY 2010.

Recommendation 15

We recommend that the OCIO improve the spreadsheet used to track security training to include a job function/responsibility for each individual that directly maps to the table containing training requirements.

OCIO Response:

"The CIO concurs with this recommendation and believes that the current spreadsheet used to track specialized security training can be improved. We will update the spreadsheet to include job function and responsibility for each individual that maps to the table containing training requirements."

Recommendation 16

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO believes that many employees are already taking meaningful and appropriate specialized training such as specialized courses offered through outside training providers, IT security conferences and other sources. However, OPM has contracted with Skills Soft to provide online training to employees at no additional cost. The CIO believes that the security courses available online through Skill Soft such as CISSP prep courses among others will be sufficient to meet the specialized training requirements."

VII. Plan of Action and Milestones Program

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&M Policy

The OCIO has developed a POA&M Guide and published it to THEO. However, the POA&M related weaknesses outlined below indicate that the OCIO has not provided adequate guidance and training to the DSO community regarding appropriate management of POA&Ms.

Recommendation 17 ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 11)***

We recommend that the OCIO work closely with the DSO community, providing training and information-sharing sessions, to implement the procedures and ensure that there is a clear understanding of the appropriate management of POA&Ms

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO is working closely with the DSO community on training and information sharing activities through the IT Security Working Group (ITSWG) that is facilitated by the Senior Agency Information Security Officer monthly. During FY10 we provided training on contingency plan testing, common security controls and POA&M management in addition to other areas. The CIO believes that this type of training is beneficial to the DSOs and for maintaining the OPM IT Security program and will continue to provide training and information sharing sessions through the ITSWG. The CIO will encourage all DSOs to take advantage of specialized training opportunities through the OPM Skill Soft program."

b) POA&Ms incorporate all known IT security weaknesses

In October 2009, the OIG issued the FY 2009 FISMA audit report with 30 audit recommendations. We verified that all 30 of the recommendations were appropriately incorporated into the OCIO POA&M.

The OIG conducted audits of three OPM systems in FY 2009 with a total of three audit recommendations that remained outstanding at the time the reports were issued. However, none of these audit recommendations appeared in the POA&M of the related system. Although each of these weaknesses has since been remediated, they should be documented in the system's POA&M for tracking purposes.

Recommendation 18 ***(Roll-Forward from OIG Reports 4A-CI-00-09-031 Recommendation 12 and 4A-CI-00-08-022 Recommendation 4)***

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO has dedicated multiple resources to ensure that all IT security weaknesses are incorporated into POA&Ms and has implemented safeguards to ensure accuracy. The CIO will continue to improve the POA&M management process."

c) Management of POA&Ms by program offices

OPM program offices are responsible for developing, implementing, and managing POA&Ms for each system that they own and operate. We were provided evidence that current POA&Ms were submitted to the OCIO on a quarterly basis for only 35 of OPM's 43 systems.

Recommendation 19 ***(Roll-Forward from OIG Reports 4A-CI-00-09-031 Recommendation 13 and 4A-CI-00-08-022 Recommendations 5 and 6)***

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

OCIO Response:

"The CIO does not concur with this recommendation. The CIO believes that up-to-date POA&Ms are in place for the systems on the OPM inventory and this is evident by a 100% compliance rate for Quarters 3 and 4 of FY10. The CIO believes that this recommendation focused on a period prior to Quarter 3 of FY10."

OIG Reply:

The OIG's review of POA&Ms did include Quarter 3 of FY 2010; three systems did not submit an up to date POA&M during this period. We continue to recommend that an up-to-date POA&M exist for each system in OPM's inventory and that system owners submit updated POA&Ms to the OCIO on a quarterly basis.

d) Remediation plans for correcting security weaknesses

When a POA&M item is remediated, OPM program offices are required to submit a work completion plan (WCP) along with evidence that the deficiency was corrected to the OCIO for review. We reviewed WCPs for eight systems and found that the majority of the program offices provided sufficient evidence that the weakness was corrected. One program office was unable to provide WCPs for closed security weaknesses and subsequently re-opened these POA&M items.

e) Compliance with estimated dates for remediation

The POA&Ms for 9 OPM systems contain security weaknesses with remediation activities over 120 days overdue. In the third quarter of 2010, OPM systems had a total of 58 POA&M items over 120 days overdue, an increase from 26 overdue items during the same time period in FY 2009.

This indicates that the OCIO has not provided adequate leadership and guidance to ensure that program offices assign reasonable POA&M due dates and stay on track to meet those dates. Program offices are equally responsible for dedicating adequate resources to addressing POA&M weaknesses and meeting target objectives.

Recommendation 20 *(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 14)*

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO agrees that an action plan to remediate POA&M weaknesses that are over 120 day is appropriate and will take steps to develop the action plan. However, the CIO does not agree that all POA&Ms that are over 120 days can be remediated immediately because the resolution to some of these POA&MS are beyond OPM's controls and require the cooperation of other stakeholders outside of OPM such as other Federal agencies. Many of these agencies for example have not implemented two factor authentication for various reasons including financial and this will prevent closure of certain POA&Ms that are over 120

days. The CIO will make every effort to assess and remediate as many of these POA&Ms as possible."

OIG Reply:

The existence of POA&M items that require action from external stakeholders may indicate an inappropriate use of the POA&M, which is intended to track action items that must be completed by the POA&M owner in order to address a security weakness.

While we acknowledge the OCIO's efforts to remediate as many overdue POA&M items as possible, we believe that this issue will continue to escalate until the OCIO addresses the problem of assigning unreasonable POA&M remediation deadlines. The drastic increase in overdue POA&M items from FY 2009 to FY 2010 indicates that the OCIO has not adequately provided leadership and guidance to ensure that program offices assign reasonable POA&M due dates.

f) OCIO tracking and reviewing of 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 closing the related POA&M.

We selected one closed POA&M item from nine OPM systems and reviewed the proof of closure documentation provided by the program offices when the POA&M items were closed. The 9 systems were selected from a universe of 48 systems and were judgmentally chosen by OIG auditors. The results of the sample test were not projected to the entire population.

Adequate proof of closure was provided for eight of the nine systems tested. Proof of closure was not available for three POA&M items selected for the ninth system, and the program office subsequently reopened these security weaknesses. The OCIO's failure to adequately review proof of closure documentation before allowing program offices to close POA&M items increases the risk that security weaknesses remain unaddressed.

Recommendation 21

We recommend that the OCIO verify that adequate proof of closure documentation exists for remediated weaknesses before allowing the program office to close POA&M items.

OCIO Response:

"The CIO does not concur with this recommendation. The POA&M management team in the Security and Privacy Group verifies that all POA&Ms submitted by Program Offices have adequate supporting evidence to close the POA&M and ensures that a proof of closure form is completed for each POA&M before closure takes place. Request to close POA&Ms with adequate documentation or completed proof of closure forms are returned to the sender."

OIG Reply:

Although the OCIO believes that adequate procedures are in place, the results of the OIG's sample test indicated that several POA&M items were, in fact, inappropriately closed without adequate proof of closure. We continue to recommend that the OCIO verify that adequate proof of closure documentation exists for remediated weaknesses before allowing the program office to close POA&M items.

g) POA&M process prioritizes IT security weaknesses

Each program office at OPM is required to prioritize IT security weaknesses on their POA&Ms to help ensure significant IT security weaknesses are addressed in a timely manner. However, we found that the OCIO did not prioritize security weaknesses on the LAN/WAN general support system.

Recommendation 22 *(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 15)*

We recommend that the program offices responsible for the LAN/WAN prioritize the system weaknesses listed on its POA&Ms.

OCIO Response:

"The CIO does not concur with this recommendation. The LAN/WAN POA&Ms are prioritized and most recently updated during the June 2010 re-certification."

OIG Reply:

The OIG verified that the June 2010 version of the LAN/WAN POA&M prioritized security weaknesses. This recommendation is closed.

VIII. Remote Access Program

The OIG evaluated OPM's remote access program by reviewing the agency's remote access and telecommuting policies and procedures and its progress in implementing the requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46 Revision 1, "Guide to Enterprise Telework and Remote Access Security."

a) Telecommuting policies and procedures

NIST SP 800-46 Revision 1 states that a telework security policy should contain the following elements:

- Which forms of remote access the organization permits;
- Which types of telework devices are permitted to use each form of remote access;
- The type of access each type of teleworker is granted;
- How user account provisioning should be handled; and

- How the organization's remote access servers are administered and how policies in those servers are updated.

Although OPM has implemented a telecommuting policy that provides guidance on the establishment, management, and maintenance of telecommuting, it does not address any of the technical elements listed above. In addition, the telecommuting policy has not been updated since 2001.

Recommendation 23

We recommend that the OCIO update its telecommuting and remote access policy in accordance with NIST SP 800-46 Revision 1 guidelines.

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The remote access policy and procedures are currently under review while new remote access methods are being tested and evaluated. Review and testing of new policy and procedures are expected to begin the second quarter FY 2011."

b) Authentication requirements

OPM utilizes a Virtual Private Network (VPN) client to provide remote users with secure access to the agency's network environment. The OPM VPN requires username and password authentication to uniquely identify users. 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.

In FY 2009, OPM required two-factor authentication for remote access in the form of RSA token devices in combination with a password. However, the agency stopped enforcing two-factor authentication in FY 2010 and users were able to authenticate with only a password. OPM has recently implemented the capability of using Personal Identity Verification (PIV) cards along with a password for two factor authentication. Although two-factor authentication is not currently enforced, OPM plans to restrict the use of single-factor authentication by October 8, 2010.

Recommendation 24

[redacted]

OCIO Response:

"The CIO does not concur with this recommendation. [redacted]

[redacted]

OIG Reply:

[redacted]

IX. Account and Identity Management Program

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

a) Account management

OPM maintains two policies regarding management of user accounts: one related to Windows network (LAN) users and the other related to mainframe users. Both policies contain procedures for creating user accounts with the appropriate level of access as well as procedures for removing access for terminated employees.

The OIG compared a list of terminated OPM employees to a list of active LAN users. Although we found that four employees maintained access after their termination date, we do not believe that this indicates a deficiency in the account management process.

b) Properly authenticating network devices

As mentioned in section IV, above, OPM uses Excel spreadsheets to maintain an inventory of hardware devices connected to its network. [redacted] However, this control was not in place during FY 2010.

Recommendation 25

We recommend that the OCIO implement [redacted]

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. [redacted]

X. Continuous Monitoring Program

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 IT Security and Privacy Policy Volume 2 states that the security controls of all systems must be tested at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and meeting the security requirements for the system.

In addition to the annual tests, OPM's infrastructure systems (LAN/WAN and Enterprise Server) are subject to additional security control tests in the form of automated vulnerability scans. Although these scans are performed routinely, the OCIO has not developed a Continuous Monitoring Policy to provide guidance on identifying high-risk security controls along with a strategy for testing them on a continuous basis. In addition, the OCIO does not have a policy to provide guidance on continuous monitoring of systems operated by a contractor on behalf of OPM (see section XII).

Recommendation 26 (*Roll-Forward from OIG Report 4A-CI-00-07-015 Recommendation 7)*

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO believes that continuous monitoring must be part of the IT Security policy updates that are now underway with assistance from the Bureau of the Public Debt. However, the CIO believes that security controls associated with continuous monitoring are documented in the Certification & Accreditation guide posted on THEO."

OIG Reply:

The Certification and Accreditation Guide states that system owners must "select security controls in the IT system to be continuously monitored" but provides no actual guidance on doing so. We continue to recommend OPM develop a Continuous Monitoring Policy that outlines a strategy for identifying information security controls that need continuous monitoring as well as procedures for conducting tests of these controls.

b) List of common security controls

NIST SP 800-53 Revision 3, "Recommended Security Controls for Federal Information Systems," provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.

Many of the applications in OPM's system inventory are housed in OPM's LAN/WAN or Enterprise Server (mainframe) general support systems (GSS). These applications inherit a significant portion of information security controls required by NIST SP 800-53 from these environments. These inherited controls are referred to as "common controls."

When the security controls of a system are subject to testing, the program office conducting the test is not required to evaluate the controls inherited from the GSS, as these controls are certified by the OCIO. However, the OCIO does not currently maintain a published list of common security controls, and individual program offices are responsible for determining which controls are inherited from a GSS, increasing the risk that certain security controls remain untested.

Recommendation 27

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO has initiated a project to established enterprise common controls under the management of the Senior Agency Information Security Officer. The IT Security Working Group has been briefed on this project and work has started with the program offices to identify common security controls and to consolidate them in a managed data repository. Enterprise common controls are expected to be in place in FY11."

XI. Contingency Planning Program

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

The OIG verified that up-to-date contingency plans exist for only 36 of the 43 systems on OPM's master system inventory. Five of 43 systems had documented contingency plans, but they were not reviewed or updated in FY 2010. The OIG was not provided with evidence that a documented contingency plan exists for the remaining two systems.

The contingency plans for 30 of OPM's 43 systems were tested in FY 2010 in full compliance with the requirements of NIST SP 800-34, Contingency Planning Guide for Information Technology Systems. Eleven of 43 system contingency plans were tested in FY 2010, but not with a scenario-based contingency plan test conducted in accordance with NIST SP 800-34 requirements. The remaining two system contingency plans were not subject to any form of contingency plan test in FY 2010.

Of the 43 systems on OPM's inventory, only 29 had both an up-to-date contingency plan ***and*** an adequate contingency plan test in FY 2010.

OPM's Information Security and Privacy Policy Volume 2 states that each system owner must "Test the contingency plan for the information system at least annually to determine the plan's effectiveness and the system's readiness to execute the plan." However, this policy does not provide instructions for conducting business impact assessments, developing contingency plans, or conducting the contingency plan test in accordance with NIST guidance.

Recommendation 28 (*Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 7*)

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO believes that the contingency plan training provided to the Designated Security Officers through the IT Security Working Group is adequate. The CIO plans to standardize the contingency plan templates to improve the quality of the testing process."

OIG Reply:

Although a brief contingency plan training session was provided at a single IT Security Working Group meeting in FY 2010, we continue to believe that the OCIO's oversight of the contingency planning program is insufficient, as evidenced by the significant number of OPM systems without an adequate contingency plan or contingency plan test.

Recommendation 29 (*Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 8*)

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO believes that having up-to-date contingency plans are important and will continue to work with the Designated Security Officers to keep plans current."

Recommendation 30 (*Roll-Forward from OIG Reports 4A-CI-00-09-031 Recommendation 9 and 4A-CI-00-08-022 Recommendation 2*)

We recommend that OPM's program offices test the contingency plans for each system on an annual basis. The contingency plans should be immediately tested for the 13 systems that were not subject to adequate testing in FY 2010.

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. Contingency plans are tested for a majority of systems on an annual basis and the records of each test is maintaining by the Security and Privacy Group. The CIO acknowledges that some systems are behind schedule (approximately 10) with their testing in 2010 and will work to ensure that all testing is completed."

XII. Program to Oversee Contractor Systems

OPM's master system inventory indicates that 11 of the agency's 43 major applications are operated by a contractor.

In prior audits, OIG has verified that the security controls of these contractor systems were tested by an OPM employee. However, in FY 2010, 7 of the 11 contractor systems were not subject to security control testing.

In addition, OPM does not have a formal policy providing the OCIO and other program offices guidance on the appropriate oversight of contractors and contractor-run systems.

Recommendation 31

We recommend that an OPM employee test information security controls for all systems operated by a contractor on an annual basis.

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO has provided guidance for testing security controls for contractor operated systems and the Security and Privacy Group has assessed security controls at the hosting facility for the IGS_LMS Learning Management System. The Security and Privacy Group plans to extend security controls testing in FY11 at other contractor facilities operating OPM systems."

Recommendation 32 (*Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 10)*

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. Policy covering oversight of contractor systems is documented in the IT Security & Privacy Handbook volume 1 that is posted on THEO. Additional related policy will be included in the policy update effort that is now in progress that will result in comprehensive IT security policies."

OIG Reply:

We were unable to locate any reference to oversight of contractor systems in Information Security and Privacy Policy Volume 1. We continue to recommend that OPM develop a policy providing guidance on adequate oversight of contractor-operated systems.

XIII. Follow-up From Prior OIG Audit Recommendations

The following sections document the results of a follow-up review of prior IT security audit recommendations issued by the OIG.

All prior audit recommendations that have not been remediated are rolled-forward with a new recommendation number in this FY 2010 FISMA audit report. A high level summary of the follow-up review can be found in Appendix I of this report.

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

Follow-up on recommendations issued in OIG Audit Report 4A-CI-00-07-015, "Audit of the Privacy Program at OPM – FY 2007"

a) 4A-CI-00-07-015 Recommendation 1
We recommend that OPM develop a comprehensive privacy policy (or a series of policies), that addresses the required areas.

FY 2010 Status
This recommendation remains open and is rolled forward as Report 4A-CI-00-10-019 Recommendation 1 (see section I, above).

b) 4A-CI-00-07-015 Recommendation 3
We recommend that OPM continue its efforts to implement encryption capabilities on laptop computers and Blackberry mobile devices.

FY 2010 Status
The OIG has been provided evidence that the OCIO encrypts all data on all mobile computers containing sensitive information; this recommendation is closed.

c) 4A-CI-00-07-015 Recommendation 4
We recommend that OPM continue its efforts to [redacted].

FY 2010 Status
This recommendation was rolled-forward until FY 2009 Report 4A-CI-00-09-031 Recommendation 24, where it was closed. However, OPM stopped enforcing t[redacted]

[redacted] in FY 2010, and this recommendation is reopened as Report 4A-CI-00-10-019 Recommendation 24 (see section VIII, above).

d) 4A-CI-00-07-015 Recommendation 7
We recommend that OPM develop policies and procedures for periodically monitoring the Agency intranet, network, and websites for inadvertent privacy vulnerabilities.

FY 2010 Status
This recommendation is rolled-forward as Report 4A-CI-00-10-019 Recommendation 26 (see section X, above).

Follow-up on recommendations issued in OIG Audit Report 4A-CI-00-09-053, "Flash Audit Alert – Information Technology Security Program at the U.S. Office of Personnel Management"

a) 4A-CI-00-09-053 Recommendation 1
We recommend that CIS correct the FY 2009 second quarter FISMA report to accurately reflect the status of OPM's IT security position as of March 1, 2009.

FY 2010 Status
This recommendation was closed in FY 2009.

b) 4A-CI-00-09-053 Recommendation 2
We recommend that CIS develop a comprehensive set of IT security policies and procedures, and a plan for updating it at least annually.

FY 2010 Status
This recommendation remains open and is rolled forward as 4A-CI-00-10-019 Recommendation 1 (see section I, above).

c) 4A-CI-00-09-053 Recommendation 3
We recommend that the OPM Director ensure that CIS has adequate resources to properly staff its IT Security and Privacy Group.

FY 2010 Status
This recommendation remains open and is rolled forward as 4A-CI-00-10-019 Recommendation 2 (see section I, above).

d) 4A-CI-00-09-053 Recommendation 4

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

FY 2010 Status
The OCIO hired a permanent Senior Agency Information Security Officer in FY 2010; this recommendation is closed.

Follow-up on recommendations issued in OIG Audit Report 4A-CI-00-09-031, "Federal Information Security Management Act Audit – FY 2009"

a) 4A-CI-00-09-031 Recommendation 1
We recommend that CIS conduct a survey of OPM program offices (particularly the Benefits Systems Group) to identify any systems that exist but do not appear on the system inventory. The systems discovered during this survey should be promptly added to the system inventory and certified and accredited.

FY 2010 Status
The OCIO is in the process of conducting a survey of program offices to identify all missing systems, but this assessment has not been completed. This recommendation remains open and is rolled forward as Report 4A-CI-00-10-019 Recommendation 33.

Recommendation 33 ***(Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 1)***

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. A survey has been distributed to identify systems used by OPM that might not be on the system inventory. The results of the survey will be used to update that system inventory as necessary."

b) 4A-CI-00-09-031 Recommendation 2
We recommend that CIS develop and maintain an inventory of all system interfaces.

FY 2010 Status
The OCIO's master system inventory now contains a listing of all known system interfaces; this recommendation is closed.

c) 4A-CI-00-09-031 Recommendation 3
We recommend that CIS develop a policy providing guidance on the development and appropriate use of MOUs and ISAs.

FY 2010 Status
The OCIO stated that the OPM Security and Privacy Policy addresses the use of MOUs and ISAs at OPM. Although this policy states that it "applies to other agencies' systems as delineated in memorandums of understanding (MOUs) and interconnection security

agreements (ISAs) with OPM," it does not provide guidance on the development and appropriate use of MOUs and ISAs. This recommendation remains open and is rolled forward as Report 4A-CI-00-10-019 Recommendation 34.

Recommendation 34 ***(Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 3)***

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

OCIO Response:

"The CIO does not concurs with this recommendation and believe that MOU and ISA policies are documented in the IT Security and Privacy Handbook volume 2 that is posted on THEO. The current MOU/ISA policies will be enhanced as part of the security policy update project."

OIG Reply:

The FY 2009 OIG FISMA audit report stated that:

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

The OCIO agreed to the recommendation to implement a policy providing guidance on the development and appropriate use of MOUs and ISAs. Since no such policy was published in FY 2010, this recommendation remains open.

d) 4A-CI-00-09-031 Recommendation 4
We recommend that CIS conduct a survey to determine how many systems owned by another agency are used by OPM.

FY 2010 Status
The OCIO is in the process of completing a survey to determine how many systems owned by other agencies are used by OPM. However, this survey was not complete as of September 30, 2010. This recommendation remains open and is rolled forward as Report 4A-CI-00-10-019 Recommendation 35.

Recommendation 35 ***(Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 4)***

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. A survey has been distributed to program offices to identify systems used by OPM that might not be on the system inventory. The results of the survey will be used to update that system inventory as necessary and to determine other systems owned by other agencies that are used by OPM."

e) 4A-CI-00-09-031 Recommendation 5
We recommend that CIS develop a policy for adequately testing the security controls of OPM's systems, and provide training to the Designated Security Officer (DSO) community related to proper security control testing.

FY 2010 Status
This recommendation remains open and is rolled forward as Report 4A-CI-00-10-019 Recommendation 9 (see section III, above).

f) 4A-CI-00-09-031 Recommendation 6 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 1)*
We recommend that OPM ensure that an annual test of security controls has been completed for all systems. [redacted].

FY 2010 Status
This recommendation remains open and is rolled forward as Report 4A-CI-00-10-019 Recommendation 10 (see section III, above).

g) 4A-CI-00-09-031 Recommendation 7
We recommend that OPM develop detailed guidance related to developing and testing the contingency plans of agency systems and provide training to the DSO community related to proper contingency planning and contingency plan testing.

FY 2010 Status
This recommendation remains open and is rolled forward to Report 4A-CI-00-10-019 Recommendation 28 (see section XI, above).

h) 4A-CI-00-09-031 Recommendation 8
We recommend that up-to-date contingency plans be developed for all agency systems.

FY 2010 Status
This recommendation remains open and is rolled forward to Report 4A-CI-00-10-019 Recommendation 29 (see section XI. above).

i) 4A-CI-00-09-031 Recommendation 9 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 2)*
We recommend that OPM's program offices test the contingency plans for each system on an annual basis.

FY 2010 Status
This recommendation remains open and is rolled forward to Report 4A-CI-00-10-019 Recommendation 30 (see section XI, above).

j) 4A-CI-00-09-031 Recommendation 10
We recommend that OPM develop a policy providing guidance on providing adequate oversight of contractor operated systems.

FY 2010 Status
This recommendation remains open and is rolled forward to Report 4A-CI-00-10-019 Recommendation 32 (see section XII, above).

k) 4A-CI-00-09-031 Recommendation 11
We recommend that CIS publish the Plan of Action and Milestone Standard Operating Procedure to THEO. Once the procedures have been published, CIS should work closely with the DSO community, providing training and information-sharing sessions, to implement the procedures and ensure that there is a clear understanding of the appropriate management of POA&Ms.

FY 2010 Status
Although the OCIO has published a POA&M Guide to THEO, adequate training has not been provided to the DSO community. This recommendation remains open and is rolled forward to Report 4A-CI-00-10-019 Recommendation 17 (see section VII, above).

l) 4A-CI-00-09-031 Recommendation 12 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 4)*
We recommend that OPM program offices incorporate all known IT security weaknesses into POA&Ms.

FY 2010 Status
This recommendation remains open and is rolled forward to Report 4A-CI-00-10-019 Recommendation 18 (see section VII, above).

m) 4A-CI-00-09-031 Recommendation 13 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendations 5 and 6)*
We recommend that an up-to-date POA&M exist for each system in OPM's inventory, and that system owners submit updated POA&Ms to CIS on a quarterly basis.

FY 2010 Status
This recommendation remains open and is rolled forward to Report 4A-CI-00-10-019 Recommendation 19 (see section VII, above).

n) 4A-CI-00-09-031 Recommendation 14

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

FY 2010 Status

This recommendation remains open and is rolled forward to Report 4A-CI-00-10-019 Recommendation 20 (see section VII, above).

o) 4A-CI-00-09-031 Recommendation 15

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

FY 2010 Status

This recommendation remains open and is rolled forward to Report 4A-CI-00-10-019 Recommendation 22 (see section VII, above).

p) 4A-CI-00-09-031 Recommendation 16 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 9)*

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

FY 2010 Status

This recommendation remains open and is rolled forward to Report 4A-CI-00-10-019 Recommendation 5 (see section III, above).

q) 4A-CI-00-09-031 Recommendation 17

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

FY 2010 Status

The FIPS Publication 199 security categorization has been corrected for the system in question; this recommendation is closed.

r) 4A-CI-00-09-031 Recommendation 18

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

FY 2010 Status

A new PIA Guide has been developed in compliance with OMB Memorandum M-03-22; this recommendation is closed.

s) 4A-CI-00-09-031 Recommendation 19

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

FY 2010 Status

The OCIO has begun the process of helping program offices complete the PIA survey that is part of the new PIA Guide. However, the surveys were not complete as of September 30, 2010. This recommendation remains open and is rolled forward as Report 4A-CI-00-10-019 Recommendation 36.

Recommendation 36 *(Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 19)*

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

OCIO Response:

"The CIO does not concur with this recommendation. A Privacy Threshold Analysis documentation is performed for each system to discover whether a PIA is required. This is in accordance with NIST 800-122 recommendations."

OIG Reply:

We confirmed that a Privacy Threshold Analysis has been conducted for each system in OPM's inventory. This recommendation is closed.

t) 4A-CI-00-09-031 Recommendation 20

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

FY 2010 Status

The OCIO has begun the process of helping program offices complete new PIAs. However, the assessments were not complete as of September 30, 2010. This recommendation remains open and is rolled forward as Report 4A-CI-00-10-019 Recommendation 37.

Recommendation 37 *(Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 20)*

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The new PIA template was reviewed and

accepted by the OIG. We are informing DSO's that there are new requirements when they submit their PIA's for review. The PIA submitted by the DSO is being updated with the new questions required by the IG and returned to the DSO for completion.

The 'guide' itself is being updated to reflect the new questions and will need to be approved in DMS through the established directive process before it can be published to the OPM.GOV and THEO websites."

u) 4A-CI-00-09-031 Recommendation 21
We recommend that each system owner annually review the existing PIA for their system to reevaluate current holdings of personally identifiable information (PII), and that they submit evidence of the review to CIS.

FY 2010 Status
Each system owner is reviewing the PIA for their system as part of the process of implementing the new PIA Guide. However, the assessments were not complete as of September 30, 2010. This recommendation remains open and is rolled forward as Report 4A-CI-00-10-019 Recommendation 38.

Recommendation 38 *(Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 21)*

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

OCIO Response:

"The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. System Owners are required to validate PTAs annually."

v) 4A-CI-00-09-031 Recommendation 22 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 12)*
We recommend that OPM continue its efforts to eliminate the unnecessary use of social security numbers (SSNs) in accordance with OMB Memorandum M-07-16.

FY 2010 Status
The OCIO has developed a plan to eliminate the unnecessary use of SSNs, but does not currently have the resources to execute the plan. The recommendation remains open and will be rolled forward as Report 4A-CI-00-10-019 Recommendation 39.

Recommendation 39 *(Roll-Forward from OIG Reports 4A-CI-00-09-031 Recommendation 22 and 4A-CI-00-08-022 Recommendation 12)*

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

OCIO Response:

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

w) 4A-CI-00-09-031 Recommendation 23
We recommend that OPM participate in government-wide efforts to explore alternatives to agency use of SSNs, as required by OMB Memorandum M-07-16.

FY 2010 Status
The OIG has been provided evidence that OPM participates in government-wide efforts to explore alternatives to agency use of SSNs; this recommendation is closed.

x) 4A-CI-00-09-031 Recommendation 24 *(Roll-Forward from OIG Reports 4A-CI-00-08-022 Recommendation 13, 4A-CI-00-07-015 Recommendation 3, and 4A-CI-00-07-007 Recommendation 4)*
We recommend that CIS encrypt all data on all mobile computers containing sensitive information.

FY 2010 Status
The OIG has been provided evidence that the OCIO encrypts all data on all mobile computers containing sensitive information; this recommendation is closed.

y) 4A-CI-00-09-031 Recommendation 25
We recommend that OPM develop an up-to-date Security Configuration and Hardening Policy, Patch Management Policy, and System Monitoring Policy.

FY 2010 Status
This recommendation remains open and is rolled forward to Report 4A-CI-00-10-019 Recommendation 11 (see section IV, above).

z) 4A-CI-00-09-031 Recommendation 26 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 16)*
We recommend that OPM implement FDCC compliant images on all OPM workstations.

FY 2010 Status
This recommendation remains open and is rolled forward to Report 4A-CI-00-10-019 Recommendation 14 (see section IV, above).

aa) 4A-CI-00-09-031 Recommendation 27
We recommend that OPM incorporate Federal Acquisition Regulation 2007-004 language in all contracts related to common security settings.

FY 2010 Status

The OCIO has taken steps towards incorporating Federal Acquisition Regulation 2007-004 language in all contracts related to common security settings, but the language does not yet appear in all contracts. The formatting of the new language is still in draft form. The recommendation remains open and is rolled forward as Report 4A-CI-00-10-019 Recommendation 40.

Recommendation 40 ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 27)***

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

OCIO Response:

"The CIO concurs with this recommendation."

bb) 4A-CI-00-09-031 Recommendation 28 *(Roll-Forward from OIG Report 4A-CI-00-08-022 Recommendation 15)*

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

FY 2010 Status

The [redacted] vulnerability in question has not been addressed as this database is currently in the process of migrating to a new version of [redacted] This recommendation remains open and is rolled forward as Report 4A-CI-00-10-019 Recommendation 41.

Recommendation 41 ***(Roll-Forward from OIG Reports 4A-CI-00-09-031 Recommendation 28 and 4A-CI-00-08-022 Recommendation 15)***

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

OCIO Response:

"The CIO concurs with this recommendation."

cc) 4A-CI-00-09-031 Recommendation 29

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

FY 2010 Status

OPM's master system inventory appropriately identifies systems that are subject to an e-Authentication risk assessment; this recommendation is closed.

dd) 4A-CI-00-09-031 Recommendation 30 *(Roll-Forward from OIG Reports 4A-CI-00-08-022 Recommendation 19, 4A-CI-00-07-007 Recommendation 3 and 9, 4A-CI-00-07-015 Recommendation 1, and 4A-CI-00-06-016 Recommendation 6)*

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

FY 2010 Status

This recommendation remains open and is rolled forward to Report 4A-CI-00-10-019 Recommendation 1 (see section I, above).

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], Lead IT Auditor
- [redacted], IT Auditor
- [redacted], IT Auditor
- [redacted], IT Auditor

Appendix I

Status of Prior OIG Audit Recommendations

The tables below outline the current status of prior audit recommendations issued by the Office of the Inspector General.

Report No. 4A-IS-00-05-026: Audit of IT Security Controls for the Electronic Questionnaire for Investigative Processing (e-QIP), issued June 16, 2005

Rec #	Original Recommendation	Recommendation History	Current Status
18	We recommend that FISD verify that only authorized users have access to e-QIP and document and maintain on file authorizations for users, including administrators, operators, and developers.	Recommendation new in FY 2005. In FY 2009 FISD was in the process of updating OPM account access request form 1665 to address this recommendation.	OPEN – OPM Form 1665 has not been updated as of September 30, 2010

Report No. 4A-CI-00-06-016: FY 2006 Federal Information Security Management Act Audit, issued September 22, 2006

Rec #	Original Recommendation	Recommendation History	Current Status
6	We recommend that the CIS/CIO develop and document a formal process to promptly analyze new and existing guidance and update OPM's IT security policies and procedure accordingly.	Recommendation new in FY 2006. Rolled-forward as Report 4A-CI-00-07-007 Recommendation 9, 4A-CI-00-08-022 Recommendation 19, and 4A-CI-00-09-031 Recommendation 30.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 1.

Report No. 4A-CI-00-07-015: FY 2007 Audit of the Privacy Program at OPM, issued January 25, 2007

Rec #	Original Recommendation	Recommendation History	Current Status
1	We recommend that OPM develop a comprehensive privacy policy (or a series of policies), that addresses the required areas.	Recommendation new in FY 2007. Rolled-forward as Report 4A-CI-00-07-007 Recommendation 3.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 1.

3	We recommend that OPM continue its efforts to implement encryption capabilities on laptop computers and Blackberry mobile devices.	Recommendation new in FY 2007. Rolled-forward as Report 4A-CI-00-07-007 Recommendation 4, 4A-CI-00-08-022 Recommendation 13, and 4A-CI-00-09-031 Recommendation 24.	CLOSED
4	We recommend that OPM [redacted].	Recommendation new in FY 2007. Rolled-forward as Report 4A-CI-00-07-007 Recommendation 4, 4A-CI-00-08-022 Recommendation 13, and 4A-CI-00-09-031 Recommendation 24.	CLOSED
7	We recommend that OPM develop policies and procedures for periodically monitoring the Agency intranet, network, and websites for inadvertent privacy vulnerabilities.	Recommendation new in FY 2007.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 26.

Report No. 4A-CI-00-07-007: FY 2007 Federal Information Security Management Act Audit, issued September 18, 2007

Rec #	Original Recommendation	Recommendation History	Current Status
3	We recommend that OPM's Plans and Policy Group continue its efforts to develop an Agency-wide privacy policy.	Rolled-forward ***from*** Report 4A-CI-00-07-015 Recommendation 1. Rolled forward ***as*** Report 4A-CI-00-08-022 Recommendation 19, and 4A-CI-00-09-031 Recommendation 30.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 1.
4	We recommend that OPM continue its efforts to protect sensitive data by implementing technical controls in compliance with OMB Memorandum M-06-16.	Rolled-forward ***from*** Report 4A-CI-00-70-015 Recommendation 3. Rolled-forward ***as*** Report 4A-CI-00-08-022 Recommendation 13, and 4A-CI-00-09-031 Recommendation 24.	CLOSED
9	We recommend that the CIS/CIO promptly update OPM's IT security policies.	Rolled-forward ***from*** Report 4A-CI-00-06-016 Recommendation 6. Rolled-forward ***as*** Report 4A-CI-00-08-022 Recommendation 19, and FY 2009 4A-CI-00-09-031 Recommendation 30.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 1.

Report No. 4A-CI-00-08-022: FY 2008 Federal Information Security Management Act Audit, issued September 23, 2008

Rec #	Original Recommendation	Recommendation History	Current Status
1	We recommend that OPM ensure that an annual test of security controls has been completed for all systems.	Recommendation new in FY 2008. Rolled-forward as Report 4A-CI-00-09-031 Recommendation 6.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 10.
2	We recommend that OPM's program offices test the contingency plans for each system on an annual basis.	Recommendation new in FY 2008. Rolled-forward as Report 4A-CI-00-09-031 Recommendation 9.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 30.
4	We recommend that the program offices incorporate all known security weaknesses into the POA&Ms.	Recommendation new in FY 2008. Rolled-forward as Report 4A-CI-00-09-031 Recommendation 12.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 18.
5	We recommend that an up-to-date POA&M exist for each system in OPM's inventory.	Recommendation new in FY 2008. Rolled-forward as Report 4A-CI-00-09-031 Recommendation 13.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 19.
6	We recommend that all program offices submit POA&Ms to the CIS/CIO office on a quarterly basis.	Recommendation new in FY 2008. Rolled-forward as Report 4A-CI-00-09-031 Recommendation 13.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 19.
9	We recommend that the CIS/CIO take the appropriate steps to ensure that all active systems in OPM's inventory have a complete and current C&A.	Recommendation new in FY 2008. Rolled-forward as Report 4A-CI-00-09-031 Recommendation 16.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 5.
12	We recommend that OPM continue its efforts to reduce the use of SSNs and develop a formal plan to eliminate the unnecessary collection and use of SSNs within 18 months in accordance with OMB M-07-16.	Recommendation new in FY 2008. Rolled-forward as Report 4A-CI-00-09-031 Recommendation 22.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 39.
13	We recommend that OPM continue its efforts to implement a solution to automatically encrypt all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive.	Rolled-forward ***from*** Report 4A-CI-00-07-007 Recommendation 4 and 4A-CI-00-07-015 Recommendation 3. Rolled forward ***as*** Report 4A-CI-00-09-031 Recommendation 24.	CLOSED

15	We recommend that OPM configure its [redacted] in a manner consistent with OPM's [redacted] Configuration Policy. Each of the vulnerabilities outlined in the OIG's audit inquiry should be formally documented, itemized, and prioritized in a POA&M. In the event that a vulnerability cannot be remediated due to a technical or business reason, the supported system's owner should document the reason in the system's ISSP to formally accept any associated risks.	Recommendation new in FY 2008. Rolled-forward as Report 4A-CI-00-09-031 Recommendation 28.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 41.
16	We recommend that OPM continue its efforts to implement all required elements of the FDCC.	Recommendation new in FY 2008. Rolled-forward as Report. 4A-CI-00-09-031 Recommendation 26.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 14.
19	We recommend that the CIS/CIO promptly update OPM's IT security policies and publish them to THEO.	Rolled-forward ***from*** Report 4A-CI-00-07-007 Recommendation 3 and 9, 4A-CI-00-07-015 Recommendation 1, and 4A-CI-00-06-016 Recommendation 6. Rolled-forward ***as*** Report 4A-CI-00-09-031 Recommendation 30.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 1.

Report No. 4A-CI-00-09-053: Flash Audit Alert – Information Technology Security Program at the U.S. Office of Personnel Management, issued May 27, 2009

FY Rec #	Flash Audit Alert Original Recommendation	Recommendation History	Current Status
1	We recommend that CIS correct the FY 2009 second quarter FISMA report to accurately reflect the status of OPM's IT security position as of March 1, 2009.	Recommendation new in FY 2009.	CLOSED
2	We recommend that CIS develop a comprehensive set of IT security policies and procedures, and a plan for updating it at least annually.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 1.
3	We recommend that the OPM Director ensure that CIS has	Recommendation new in FY 2009.	OPEN – Rolled-forward as

	adequate resources to properly staff its IT Security and Privacy Group.		Report 4A-CI-00-10-019 Recommendation 2.
4	We recommend that CIS recruit a permanent Senior Agency Information Security Officer as soon as possible, and adequate staff to effectively manage the agency's IT security program.	Recommendation new in FY 2009.	CLOSED

Report No. 4A-HR-00-09-033: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Enterprise Human Resources Integration Data Warehouse FY 2009, issued June 1, 2009

Rec #	Original Recommendation	Recommendation History	Current Status
1	We recommend that HRLOB routinely audit active EHRIDW user accounts for appropriateness.	Recommendation new in FY 2009.	CLOSED

Report No. 4A-CI-00-09-052: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Integrated Security Management System, issued August 10, 2009

Rec #	Original Recommendation	Recommendation History	Current Status
1	We recommend that CSEA continue to develop and improve the ISMS contingency plan. This includes, but is not limited to, adding specific and detailed steps to the recovery procedures and assigning specific individuals to the various recovery teams. CSEA should conduct another test of the contingency plan after the plan has been modified.	Recommendation new in FY 2009.	CLOSED
2	We recommend that ISMS edit its POA&M template to facilitate the prioritization of weaknesses.	Recommendation new in FY 2009.	CLOSED
3	We recommend that CSEA expand the ISMS audit procedures to include a process for reviewing the activities of the system administrator.	Recommendation new in FY 2009.	CLOSED

4	We recommend that CSEA disable all shared user accounts for ISMS, and enforce the use of individual accounts for all users.	Recommendation new in FY 2009.	CLOSED
5	We recommend that CSEA document a baseline configuration for ISMS's application level settings and develop procedures for requesting and approving changes to these settings.	Recommendation new in FY 2009.	CLOSED
6	We recommend that CSEA have all ISMS users sign the rules of behavior document.	Recommendation new in FY 2009.	CLOSED

Report No. 4A-CI-00-09-031: FY 2009 Federal Information Security Management Act Audit, issued November 4, 2009

FY Rec #	Original Recommendation	Recommendation History	Current Status
1	We recommend that CIS conduct a survey of OPM program offices (particularly the Benefits Systems Group) to identify any systems that exist but do not appear on the system inventory. The systems discovered during this survey should be promptly added to the system inventory and certified and accredited.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 33.
2	We recommend that CIS develop and maintain an inventory of all system interfaces.	Recommendation new in FY 2009.	CLOSED
3	We recommend that CIS develop a policy providing guidance on the development and appropriate use of MOUs and ISAs.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 34.
4	We recommend that CIS conduct a survey to determine how many systems owned by another agency are used by OPM.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 35.
5	We recommend that CIS develop a policy for adequately testing the security controls of OPM's systems, and provide training to the Designated Security Officer (DSO) community related to proper security control testing.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 9.

6	We recommend that OPM ensure that an annual test of security controls has been completed for all systems. The IT security controls should be immediately tested for the two systems that were not subject to testing in FY 2009.	Rolled-forward from Report 4A-CI-00-08-022 Recommendation 1.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 10.
7	We recommend that OPM develop detailed guidance related to developing and testing the contingency plans of agency systems and provide training to the DSO community related to proper contingency planning and contingency plan testing.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 28.
8	We recommend that up-to-date contingency plans be developed for all agency systems.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 29.
9	We recommend that OPM's program offices test the contingency plans for each system on an annual basis. The contingency plans should be immediately tested for the 11 systems that were not subject to testing in FY 2009.	Rolled-forward from Report 4A-CI-00-08-022 Recommendation 2.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 30.
10	We recommend that OPM develop a policy providing guidance on providing adequate oversight of contractor operated systems.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 32.
11	We recommend that CIS publish the Plan of Action and Milestone Standard Operating Procedure to THEO. Once the procedures have been published, CIS should work closely with the DSO community, providing training and information-sharing sessions, to implement the procedures and ensure that there is a clear understanding of the appropriate management of POA&Ms.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 17.
12	We recommend that OPM program offices incorporate all known IT security weaknesses into POA&Ms.	Rolled-forward from Report 4A-CI-00-08-022 Recommendation 4.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 18.
13	We recommend that an up-to-date POA&M exist for each system in OPM's inventory, and that system owners submit updated POA&Ms to CIS on a quarterly basis.	Rolled-forward from Report 4A-CI-00-08-022 Recommendations 5 and 6.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 19.

14	We recommend that CIS develop a formal corrective action plan to immediately remediate all POA&M weaknesses that are over 120 days overdue. In addition, we recommend that CIS take a lead role in the future and work closely with OPM program offices to ensure that POA&M completion dates are achieved.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 20.
15	We recommend that the program offices responsible for the two systems in question prioritize the system weaknesses listed on their POA&Ms.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 22.
16	We recommend that all active systems in OPM's inventory have a complete and current C&A.	Rolled-forward from Report 4A-CI-00-08-022 Recommendation 9.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 5.
17	We recommend that the FIPS Publication 199 security categorization be updated for the inappropriately categorized system.	Recommendation new in FY 2009.	CLOSED
18	We recommend that CIS update the PIA Guide to address all of the requirements of OMB Memorandum M-03-22.	Recommendation new in FY 2009.	CLOSED
19	We recommend that CIS conduct a new PIA survey to determine which OPM systems require a PIA, including those systems that process sensitive information about government employees and contractors.	Recommendation new in FY 2009.	CLOSED - Rolled-forward as Report 4A-CI-00-10-019 Recommendation 36, but closed due to response from draft report.
20	We recommend that a new PIA be conducted for the appropriate systems based on the updated PIA Guide.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 37.
21	We recommend that each system owner annually review the existing PIA for their system to reevaluate current holdings of PII, and that they submit evidence of the review to CIS.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 38.
22	We recommend that OPM continue its efforts to eliminate the unnecessary use of SSNs in accordance with OMB Memorandum M-07-16.	Rolled-forward from Report 4A-CI-00-08-022 Recommendation 12.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 39.
23	We recommend that OPM participate in government-wide efforts to explore alternatives to agency use of SSNs, as	Recommendation new in FY 2009.	CLOSED

	required by OMB Memorandum M-07-16.		
24	We recommend that CIS encrypt all data on all mobile computers containing sensitive information.	Rolled-forward from Report 4A-CI-00-07-007 Recommendation 4, 4A-CI-00-07-015 Recommendation 3, and Report 4A-CI-00-08-022 Recommendation 13.	CLOSED
25	We recommend that OPM develop an up-to-date Security Configuration and Hardening Policy, Patch Management Policy, and System Monitoring Policy.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 11.
26	We recommend that OPM implement FDCC compliant images on all OPM workstations.	Rolled-forward from Report 4A-CI-00-08-022 Recommendation 16.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 14.
27	We recommend that OPM incorporate Federal Acquisition Regulation 2007-004 language in all contracts related to common security settings.	Recommendation new in FY 2009.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 40.
28	We recommend that in the event that an [redacted] vulnerability cannot be remediated due to a technical or business reason, the system's owner should document the reason in the system's ISSP and formally accept any associated risks.	Rolled-forward from Report 4A-CI-00-08-022 Recommendation 15.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 41.
29	We recommend that CIS determine which systems in its inventory are subject to e-Authentication requirements and complete e-Authentication risk assessments for each of these systems.	Recommendation new in FY 2009.	CLOSED
30	We recommend that CIS develop up-to-date and comprehensive IT security policies and procedures, and publish these documents to THEO.	Rolled-forward from Report 4A-CI-00-06-016 Recommendation 6, 4A-CI-00-07-007 Recommendation 3 and Recommendation 9, 4A-CI-00-07-015 Recommendation 1, and 4A-CI-00-08-022 Recommendation 19.	OPEN – Rolled-forward as Report 4A-CI-00-10-019 Recommendation 1.

Appendix II

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Information Officer

MEMORANDUM FOR [redacted]
Chief, Information Systems Audit Group

FROM: MATTHEW E. PERRY
Chief Information Officer
10/07/2010

Subject: Response to the Federal Information Security Management Act Audit – FY2010, Report NO. 4A-CI-00-10-019

Thank you for the opportunity to comment on the subject report. The results provided in the draft report consist of a number of recommendations. The recommendations are valuable to our program improvement efforts and most of them are generally consistent with our plan.

OIG Recommendations:

Recommendation 1 ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 30, 4A-CI-00-08-022 Recommendation 19, and 4A-CI-00-09-053 Recommendation 2)***

We recommend that CIS develop up-to-date and comprehensive IT security policies and procedures, and publish these documents to THEO, and a plan for updating them at least annually.

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation of the status of the IT security policies and procedures. The IT security and privacy policy volumes 1 and volume 2 were last updated and posted on THEO in August 2009. The CIO understands that additional policy updates are required to comply with guidance issued by NIST during the last year and to address some deficiencies in the current policies. The Bureau of the Public Debt (BPD) has been retained through an Interagency Agreement to update and to bring IT Security and Privacy policies into OPM and FISMA compliance. A kickoff meeting was held for this project on September 2010 and BPD is expected to be on site to collect policy requirements during the next 60 days. A comprehensive IT security and Privacy handbook is expected to be completed in FY2011.

This recommendation also cited the need for procedures and a number of procedures were created or updated and posted on THEO in 2009/2010 including:

- Certification and Accreditation Guide (July 2009)
- Incident Response and Reporting Guide (July 2009)
- LAN Complex Passwords (June 2009)
- OPM Computer User Responsibilities (June 2009)

- Plan of Action and Milestone (POA&M Standard Operating Procedure (September 2009)
- Process for Analyzing New and Emerging Information Security and Privacy Requirements (July 2009)
- System Access Authorization Procedure (July 2009)
- Privacy Impact Assessment (PIA) Guide (April 2010)
- System of Records Notice (SORN) Guide (April 2010)

The CIO believes that the above procedures have enhanced IT security and privacy at OPM and understands that additional work needs to be done to develop new procedures and to enhance existing ones as necessary. Current procedures will be revisited and additional ones will be developed in FY2011 as necessary.

Recommendation 2 ***(Roll-forward from OIG Report 4A-CI-00-09-053 Recommendation 3)***

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation of the staffing situation in the IT Security and Privacy Group. During the past five months, a Senior Agency Information Security Officer has being hired and the staff complement in the security and privacy group has increased from [redacted] FTEs along with contractor resources as needed. Recognizing that additional staff resources are needed, the CIO believes that incremental progress is being made in this area.

Recommendation 3

We recommend that CIO develop and implement an active strategy to maintain up-to-date information regarding OPM's master system inventory.

The CIO concurs with this recommendation and has already taken steps through the issuance of a data call to the IT Security Working Group on September 8, 2010 to identify systems used by OPM that are not on the FISMA system inventory. The CIO has also initiated an internal review to determine if applications were inappropriately bundled into other larger systems as previously reported in prior audit findings. Additional systems identified from the data call and internal system review will be evaluated for addition to the master system inventory.

Recommendation 4

We recommend that OPM implement a centralized information security governance structure where all information security practitioners, including designated security officers, report to the Senior Agency Information Security Official. Adequate resources

should be assigned to the OCIO to create this structure. Existing designated security officers who report to their program offices should return to their program office duties. The new staff that reports to the SAISO should consist of experienced information security professionals.

The CIO concurs with this recommendation. The overall IT security governance at OPM can be improved by implementing a centralized information security governance structure consisting of IT security professionals.

Recommendation 5 ***(Roll-Forward from OIG Report No. 4A-CI-00-09-031 Recommendation 16)***

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. Program offices are responsible for the security and C&A of their systems. C&As are often contracted to various entities that employ different styles in preparing the final packages and this explains why all C&A packages do not look alike. The CIO believes that all completed C&A packages must properly address required security controls and contain required artifacts per the OPM C&A Guide, and that the look and feel of packages is a reflection of the various sources contracted by the program offices to complete the packages.

Regarding, the six systems with expired C&A, the CIO agrees that all production systems should have a current C&A. However, the OPM procurement process can be lengthy depending on workload has an effect on getting contracts and interagency agreements for C&A in place. The extended Authority to Operate for the six systems was issued in support of OPM mission support activities.

Recommendation 6

We recommend that CIO develop a risk assessment policy to provide guidance to program offices conducting a risk assessment as part of the C&A process.

The CIO does not concur with this recommendation. Risk assessment policies are documented in the current IT security and Privacy policy volume 2 that is posted on THEO. However, risk assessment policy will be revisited and updated in the new IT Security policy updates that BPD has been retained to complete.

Recommendation 7

We recommend that CIO develop an ISSP policy to provide guidance to program offices developing a security plan as part of the C&A process.

The CIO does not concur with this recommendation. Information Systems Security Plan policies are documented in the current IT security and Privacy policy volume 2 that is posted on THEO. The policies also references NIST security plan templates that can be used to build a security plan. However, IT security plans policy will be updated to provide additional as part of the BPD policy update project.

Regarding the review of C&A packages, two full time resources have been hired to review C&A packages and to provide guidance to the DSO community. One of these resources is already onboard and the second is expected to start work after completing the necessary new employee onboarding procedures.

Recommendation 8

We recommend that CIO assign additional resources to facilitate the C&A process to ensure the consistency and quality of C&A packages developed by OPM program offices.

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO has doubled the number of full time resources assigned to the C&A program and this increase in resources will improve the quality of C&A packages. C&A packages found to be of poor quality are being returned to for rework for correction of deficiencies.

Recommendation 9 *(Roll-Forward from OIG Report No. 4A-CI-00-09-031 Recommendation 5)*

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The Information Security and Privacy Policy Volume 1 requires security controls to be Periodically assessed and CIO security staff works with the DSO community on annual testing efforts including keeping track of the number of systems that have tested their security controls. We will enhance the current security policy in the security

handbook that is under development and provide additional guidance to DSOs to enhance the testing of security controls.

Recommendation 10 ***(Roll-Forward from OIG Report No. 4A-CI-00-09-031 Recommendation 6 and Report 4A-CI-00-08-022 Recommendation 1)***

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO staff continues works with the DSO community to ensure that security controls have been tested for all systems. The CIO security staff sends out a reminder to all DSOs each month informing them to complete required security controls testing and assist with technical guidance. We will continue to work with the DSO community and escalate systems where security controls have not been tested to the associated director in the specific business area.

Recommendation 11 ***(Roll-Forward from OIG Report No. 4A-CI-00-09-031 Recommendation 25)***

We recommend that CIO develop and publish to THEO an up-to-date Patch Management Policy.

The CIO does not concur with this recommendation. The OPM ISPP details the high level patch (flaw remediation) requirements and agency policy. (See ISPP Volume 2, page 71. 800-53 rev 3 Control SI-2). Low level procedures exist and are utilized by the Network Management administrators to patch desktops and servers. Ongoing improvements to the patch management process are being tested and implemented as new tools and processes become available. Current initiatives include procurement requests for enterprise-wide patch and vulnerability management tools (Big Fix and Window SUS) scheduled for implementation in FY 2011.

Recommendation 12

We recommend that CIO develop a single centralized agency-wide hardware inventory.

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. Network Management is actively implementing a centralized agency-wide automated hardware inventory tracking system. Asset tags are being applied to all accountable IT assets and pending procurements for scanning equipment are expected to quickly bring the outstanding inventory under control. Daily and weekly automated inventory reports are now being produced and internal audits of the process will begin this quarter.

Recommendation 13

We recommend that CIO develop and implement a strategy for using automated techniques for tracking hardware inventory.

The CIO concurs with this recommendation.

Recommendation 14 ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 26 and Report 4A-CI-00-08-022 Recommendation 16)***

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

The CIO concurs with this recommendation and offers the following clarifying remarks: An FDCC workstation baseline image has been created and is currently being deployed. All new workstations and all agency laptops are currently secured utilizing an FDCC (USGBC) compliant image. The FDCC image has been rolled out to 1200 laptops and 800 desktops as of this date. Image deployment and enforcement of the legacy workstations is currently an active project and is being pushed through domain GPO. The addition of workstations occurs daily and is scheduled to have full completion by the end of the first quarter of FY 2011. Part of the delay in implementation was due to working with the union to assess the impact on employees.

Recommendation 15

We recommend that CIO improve the spreadsheet used to track security training to include a job function/responsibility for each individual that directly maps to the table containing training requirements.

The CIO concurs with this recommendation and believes that the current spreadsheet used to track specialized security training can be improved. We will update the spreadsheet to include job function and responsibility for each individual that maps to the table containing training requirements.

Recommendation 16

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO believes that many employees are already taking meaningful and appropriate specialized training such as specialized courses offered through outside training providers, IT security conferences and other sources. However, OPM has contracted with Skills Soft to provide online training to employees at no additional cost. The CIO believes that the security courses available online through Skill Soft such as CISSP prep courses among others will be sufficient to meet the specialized training requirements.

Recommendation 17 ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 11)***

We recommend that CIO work closely with the DSO community, providing training and information-sharing sessions, to implement the procedures and ensure that there is a clear understanding of the appropriate management of POA&Ms.

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO is working closely with the DSO community on training and information sharing activities through the IT Security Working Group (ITSWG) that is facilitated by the Senior Agency Information Security Officer monthly. During FY10 we provided training on contingency plan testing, common security controls and POA&M management in addition to other areas. The CIO believes that this type of training is beneficial to the DSOs and for maintaining the OPM IT Security program and will continue to provide training and information sharing sessions through the ITSWG. The CIO will encourage all DSOs to take advantage of specialized training opportunities through the OPM Skill Soft program.

Recommendation 18 ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 12 and OIG Report 4A-CI-00-08-022 Recommendation 4)***

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO has dedicated multiple resources to ensure that all IT security weaknesses are incorporated into POA&Ms and has implemented safeguards to ensure accuracy. The CIO will continue to improve the POA&M management process.

Recommendation 19 ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 13 and 4A-CI-00-08-022 Recommendations 5 and 6)***

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

The CIO does not concur with this recommendation. The CIO believes that up-to-date POA&Ms are in place for the systems on the OPM inventory and this is evident by a 100% compliance rate for Quarters 3 and 4 of FY10. The CIO believes that this recommendation focused on a period prior to Quarter 3 of FY10.

Recommendation 20 (*Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 14)*

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO agrees that an action plan to remediate POA&M weaknesses that are over 120 day is appropriate and will take steps to develop the action plan. However, the CIO does not agree that all POA&Ms that are over 120 days can be remediated immediately because the resolution to some of these POA&MS are beyond OPM's controls and require the cooperation of other stakeholders outside of OPM such as other Federal agencies. Many of these agencies for example have not implemented two factor authentication for various reasons including financial and this will prevent closure of certain POA&Ms that are over 120 days. The CIO will make every effort to assess and remediate as many of these POA&Ms as possible.

Recommendation 21

We recommend that CIO verify that adequate proof of closure documentation exists for remediated weaknesses before allowing the program office to close POA&M items.

The CIO does not concur with this recommendation. The POA&M management team in the Security and Privacy Group verifies that all POA&Ms submitted by Program Offices have adequate supporting evidence to close the POA&M and ensures that a proof of closure form is completed for each POA&M before closure takes place. Request to close POA&Ms with adequate documentation or completed proof of closure forms are returned to the sender.

Recommendation 22 (*Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 15)*

We recommend that the program offices responsible for the LAN/WAN prioritize the system weaknesses listed on its POA&Ms.

The CIO does not concur with this recommendation. The LAN/WAN POA&Ms are prioritized and most recently updated during the June 2010 re-certification.

Recommendation 23

We recommend that CIO update its telecommuting and remote access policy in accordance with NIST SP 800-46 Revision 1 guidelines.

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The remote access policy and procedures are currently under review while new remote access methods are being tested and evaluated. Review and testing of new policy and procedures are expected to begin the second quarter FY 2011.

Recommendation 24

We recommend that CIO [redacted]

The CIO does not concur with this recommendation. [redacted]

Recommendation 25:

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. An automated process to detect unauthenticated network devices has been procured and is expected to be in place and operational in the third quarter FY 2011.

Recommendation 26

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO believes that continuous monitoring must be part of the IT Security policy updates that are now underway with assistance from the Bureau of the Public Debt. However, the CIO believes that security controls associated with continuous monitoring are documented in the Certification & Accreditation guide posted on THEO.

Recommendation 27

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO has initiated a project to established enterprise common controls under the management of the Senior Agency Information Security Officer. The IT Security Working Group has been briefed on this project and work has started with the program offices to identify common security controls and to consolidate them in a managed data repository. Enterprise common controls are expected to be in place in FY11.

Recommendation 28 ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 7)***

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO believes that the contingency plan training provided to the Designated Security Officers through the IT Security Working Group is adequate. The CIO plans to standardize the contingency plan templates to improve the quality of the testing process.

Recommendation 29: ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 8)***

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO believes that having up-to-date contingency plans are important and will continue to work with the Designated Security Officers to keep plans current.

Recommendation 30: ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 9 and OIG Report 4A-CI-00-08-022 Recommendation 2)***

We recommend that OPM's program offices test the contingency plans for each system on an annual basis. The contingency plans should be immediately tested for the 17 systems that were not subject to adequate testing in FY 2010.

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. Contingency plans are tested for a majority of systems on an annual basis and the records of each test is maintaining by the Security and Privacy Group. The CIO acknowledges that some systems are behind schedule (approximately 10) with their testing in 2010 and will work to ensure that all testing is completed.

Recommendation 31

We recommend that an OPM employee test information security controls for all systems operated by a contractor on an annual basis.

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The CIO has provided guidance for testing security controls for contractor operated systems and the Security and Privacy Group has assessed security controls at the hosting facility for the IGS_LMS Learning Management System. The Security and Privacy Group plans to extend security controls testing in FY11 at other contractor facilities operating OPM systems.

Recommendation 32 ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 10)***

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. Policy covering oversight of contractor systems is documented in the IT Security & Privacy Handbook volume 1 that is posted on THEO. Additional related policy will be included in the policy update effort that is now in progress that will result in comprehensive IT security policies.

Recommendation 33 ***(Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 1)***

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. A survey has been distributed to identify systems used by OPM that might not be on the system inventory. The results of the survey will be used to update that system inventory as necessary.

Recommendation 34 ***(Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 3)***

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

The CIO does not concurs with this recommendation and believe that MOU and ISA policies are documented in the IT Security and Privacy Handbook volume 2 that is posted on THEO. The current MOU/ISA policies will be enhanced as part of the security policy update project.

Recommendation 35 ***(Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 4)***

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. A survey has been distributed to program offices to identify systems used by OPM that might not be on the system inventory. The results of the survey will be used to update that system inventory as necessary and to determine other systems owned by other agencies that are used by OPM.

Recommendation 36 ***(Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 19)***

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

The CIO does not concur with this recommendation. A Privacy Threshold Analysis documentation is performed for each system to discover whether a PIA is required. This is in accordance with NIST 800-122 recommendations.

Recommendation 37 ***(Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 20)***

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. The new PIA template was reviewed and accepted by the OIG. We are informing DSO's that there are new requirements when they submit their PIA's for review. The PIA submitted by the DSO is being updated with the new questions required by the IG and returned to the DSO for completion.
The "guide" itself is being updated to reflect the new questions and will need to be approved in DMS through the established directive process before it can be published to the OPM.GOV and THEO websites.

Recommendation 38 ***(Roll-forward from OIG Report 4A-CI-00-09-031 Recommendation 21)***

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

The CIO concurs with this recommendation and offers clarifying remarks in order to present a more current interpretation. System Owners are required to validate PTAs annually.

Recommendation 39 ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 22 and Report 4A-CI-00-08-022 Recommendation 12)***

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

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

Recommendation 40 ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 27)***

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

The CIO concurs with this recommendation.

Recommendation 41 ***(Roll-Forward from OIG Report 4A-CI-00-09-031 Recommendation 28 and Report 4A-CI-00-08-022 Recommendation 15)***

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

The CIO concurs with this recommendation.

cc: [redacted]
Senior Agency Information Security Officer

[redacted]
Director
Internal Oversight and Compliance

[redacted]
Chief, Policy and Internal Control

Inspector General

Section Report

2010

Annual FISMA Report

Office of Personnel Management

Printed: October 29, 2010, 8:15 am

Section 1: Status of Certification and Accreditation Program

1. Selected response is:

b. The Agency has established and is maintaining a certification and accreditation program. However, the Agency needs to make significant improvements as noted below.

Comments:

The OIG's FY 2008 and FY 2009 FISMA audit reports stated that weaknesses in OPM's C&A process were a significant deficiency in the internal control structure of the agency's IT security program. The weaknesses cited related to inadequate management of the process and incomplete, inconsistent, and poor quality C&A products. In FY 2010 these longstanding conditions not only continued, but actually degraded. As a result, we are now reporting a material weakness in the IT security control structure related to OPM's C&A process.

We believe that the root causes of these issues include insufficient staffing in the IT Security and Privacy Group, a lack of policy and procedures, and the decentralized designated security officer (DSO) model in place at OPM.

1a. Areas for Improvement:

1a(1). Certification and accreditation policy is not fully developed.

Yes

Comments:

In July 2009, OPM's Office of the Chief Information Officer (OCIO) published an agency-wide Certification and Accreditation Guide. The C&A Guide addresses the roles and responsibilities of key personnel, a walkthrough of the C&A Process, and a listing of the various security documents that are required elements of a C&A.

However, OPM's C&A Guide does not provide standard forms, templates, or detailed guidance on how to prepare each of the required elements. The lack of such guidance has led to extreme inconsistencies in the quality of C&A packages for various OPM systems.

1a(2). Certification and accreditation procedures are not fully developed, sufficiently detailed or consistently implemented.

Yes

Section 1: Status of Certification and Accreditation Program

Comments: The OIG reviewed the full C&A packages of 15 systems that were subject to a C&A during FY 2010. Although the packages we reviewed contained all of the elements required by OPM's C&A Guide, the quality of these packages varied significantly between systems.

Although various forms of general guidance are available to assist program offices in the development of C&A elements, the OCIO has not implemented centralized policies, guidelines, or templates outlining how various C&A elements should be completed for OPM systems. As a result, the content and quality of a specific C&A element varies widely between systems.

1a(3). **Information systems are not properly categorized (FIPS 199/SP 800-60).**

No

1a(4). **Accreditation boundaries for agency information systems are not adequately defined.**

No

1a(5). **Minimum baseline security controls are not adequately applied to information systems (FIPS 200/SP 800-53).**

No

1a(6). **Risk assessments are not adequately conducted (SP 800-30).**

Yes

Comments: OPM's OCIO has not developed an risk assessment policy. The extreme range in quality between risk assessments conducted by various OPM program offices indicates that the OCIO has not provided adequate risk assessment guidance.

1a(7). **Security control baselines are not adequately tailored to individual information systems (SP 800-30).**

No

1a(8). **Security plans do not adequately identify security requirements (SP 800-18).**

Yes

Comments: OPM's OCIO has not developed an information system security plan (ISSP) policy. The extreme range in quality between ISSPs conducted by various OPM program offices indicates that the OCIO has not provided adequate ISSP guidance.

1a(9). **Inadequate process to assess security control effectiveness (SP800-53A).**

Yes

Section 1: Status of Certification and Accreditation Program

Comments:

The OIG conducted a review of the documentation resulting from the security controls tests for each of the 43 systems in OPM's inventory. Our evaluation indicated that the IT security controls had been adequately tested for only 28 of OPM's 43 systems during FY 2010.

There was a wide range of quality amongst the 28 security control tests that were conducted. Some program offices tested all security controls applicable to that system while others tested only a small subset. There was also a variance in the security controls that program offices assumed to be "common controls" inherited from OPM's IT and facility infrastructures. In addition, the tests were documented in many different formats and templates. We believe that these inconsistencies are a result of OPM's lack of agency-wide policy or guidance on how to adequately test information system security controls.

1a(10). **Inadequate process to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate (SP 800-37).**

Yes

Comments:

Seven OPM systems are currently operating without an active C&A.

The OIG identified one OPM system that was in production for several years without being subject to a C&A.

In addition, the prior C&A for six additional systems from OPM's inventory expired in FY 2010, and a new C&A has not been completed. Although an "Interim Authorization to Operate" (IATO) was issued for these systems, they are currently running in a production environment without an active C&A.

1a(11). **Inadequate process to continuously track changes to information systems that may necessitate reassessment of control effectiveness (SP 800-37).**

No

1a(12). **Other**

Yes

Explanation for Other

OCIO management of C&A Process

Section 1: Status of Certification and Accreditation Program

Comments: OPM's OCIO is responsible for assisting program offices in the development of C&A packages for their systems. OPM's C&A Guide also states that the OCIO must review completed C&A packages for quality and completeness before recommending the system for accreditation.

Although the OCIO has procedures for conducting post-completion reviews of C&A packages, the OCIO does not have the resources available to actively participate in the planning or development of the C&A packages for each agency system.

Section 2: Status of Security Configuration Management

2. Selected response is:

b. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.

Comments: OPM's OCIO has implemented an agency-wide Configuration Management Policy. This policy was updated during FY 2010 and outlines the process for maintaining a secure configuration network environment.

2a. Areas for Improvement:

2a(1). Configuration management policy is not fully developed.

No

2a(2). Configuration management procedures are not fully developed or consistently implemented.

No

2a(3). Software inventory is not complete (NIST 800-53: CM-8).

No

2a(4). Standard baseline configurations are not identified for all software components (NIST 800-53: CM-8).

No

2a(5). Hardware inventory is not complete (NIST 800-53: CM-8).

Yes

Section 2: Status of Security Configuration Management

Comments: OPM currently uses several Excel spreadsheets to track its computer hardware inventory. These spreadsheets are manually updated when new hardware is purchased or old hardware is decommissioned. Separate spreadsheets are maintained by different individuals for Windows severs, Linux servers, and all servers operated by OPM's Federal Investigative Services program office. However, each of these spreadsheets is maintained independently from the other inventories, and no individual at OPM maintains a single inventory listing that contains all computer hardware owned by the agency. Therefore, the OCIO is unable to attest that all computer hardware in OPM's operating environment is accounted for.

2a(6). **Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).**

No

2a(7). **Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).**

No

2a(8). **FDCC is not fully implemented (OMB) and/or all deviations are not fully documented.**

Yes

Comments: OPM has developed a Windows XP standard image that is generally compliant with Federal Desktop Core Configuration (FDCC) standards, and has documented nine deviations between this image and FDCC requirements. However, as of September 30, 2010, OPM's FDCC compliant image has not been rolled out to the majority of OPM workstations.

2a(9). **Software scanning capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).**

No

2a(10). **Configuration-related vulnerabilities have not been remediated in a timely manner (NIST 800-53: CM-4, CM-6, RA-5, SI-2).**

No

2a(11). **Patch management process is not fully developed (NIST 800-53: CM-3, SI-2).**

Yes

Comments: OPM's OCIO has implemented a patch management policy that outlines the responsibilities and procedures for ensuring that OPM servers are routinely patched. However, this policy has not been updated since August 2005. In August 2010, the OCIO informed the OIG that this policy is in the process of being updated.

2a(12). **Other**

No

3. **Identify baselines reviewed:**

Section 2: Status of Security Configuration Management

Operating System
[redacted]

Section 3: Status of Incident Response & Reporting Program

4. Selected response is:

a. The Agency has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1. Documented policies and procedures for responding and reporting to incidents.
2. Comprehensive analysis, validation and documentation of incidents.
3. When applicable, reports to US-CERT within established timeframes.
4. When applicable, reports to law enforcement within established timeframes.
5. Responds to and resolves incidents in a timely manner to minimize further damage.

Comments:	OPM has developed an "Incident Response and Reporting Guide" that outlines the responsibilities of OPM's Computer Incident Response Team (CIRT) and documents procedures for reporting all IT security events to the appropriate entities. OPM appropriately reports security incidents internally, to US-CERT, and to law enforcement.

Section 4: Status of Security Training Program

5. Selected response is:

b. The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below.

Section 4: Status of Security Training Program

Comments: OPM's OCIO has implemented a process to provide annual IT security and privacy awareness training to all OPM employees and contractors.

Over 99 percent of OPM's employees and contractors completed the security awareness training course in FY 2010. However, only 87 percent of employees with security responsibility took specialized security training in FY 2010.

5a. Areas for Improvement:

5a(1). Security awareness training policy is not fully developed.

No

5a(2). Security awareness training procedures are not fully developed, sufficiently detailed or consistently implemented.

No

5a(3). Specialized security training policy is not fully developed.

Yes

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

OPM's OCIO has issued 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. However, a significant portion (33 percent) of the individuals on the spreadsheet are listed with a job role that does not appear on the training requirements table (i.e., "significant responsibility"), making it impossible to determine whether these individuals received adequate training in FY 2010.

5a(4). Specialized security training procedures are not fully developed or sufficiently detailed (SP 800-50, SP 800-53).

Yes

Comments: See comments in 5a(3).

5a(5). Training material for security awareness training does not contain appropriate content for the Agency (SP 800-50, SP 800-53).

No

5a(6). Identification and tracking of employees with login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).

No

Section 4: Status of Security Training Program

5a(7). **Identification and tracking of employees without login privileges that require security awareness training is not adequate (SP 800-50, SP 800-53).**

No

5a(8). **Identification and tracking of employees with significant information security responsibilities is not adequate (SP 800-50, SP 800-53).**

Yes

Comments: See comments in 5a(3).

5a(9). **Training content for individuals with significant information security responsibilities is not adequate (SP 800-53, SP 800-16).**

No

5a(10). **Less than 90% of employees with login privileges attended security awareness training in the past year.**

No

5a(11). **Less than 90% of employees, contractors, and other users with significant security responsibilities attended specialized security awareness training in the past year.**

Yes

Comments: Eighty-seven percent of OPM's employees identified as having information security responsibility have completed at least one hour of specialized security training in FY 2010.

5a(12). **Other**

No

Section 5: Status of Plans of Actions & Milestones (POA&M) Program

6. **Selected response is:**

b. The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.

6a. **Areas for Improvement:**

6a(1). **POA&M Policy is not fully developed.**

No

6a(2). **POA&M procedures are not fully developed, sufficiently detailed or consistently implemented.**

Yes

Section 5: Status of Plans of Actions & Milestones (POA&M) Program

Comments: OPM's OCIO has developed a POA&M Guide and published it to the agency's internal website. However, the OIG identified several POA&M related weaknesses that indicate that the OCIO has not provided adequate procedure guidance and training regarding appropriate management of POA&Ms.

6a(3). POA&Ms do not include all known security weaknesses (OMB M-04-25).

Yes

Comments: In October 2009, the OIG issued the FY 2009 FISMA audit report with 30 audit recommendations. We verified that all 30 of the recommendations were appropriately incorporated into the OCIO POA&M.

The OIG conducted audits of three OPM systems in FY 2009 with a total of three audit recommendations that remained outstanding at the time the reports were issued. However, none of these audit recommendations appeared in the POA&M of the related system. Although each of these weaknesses has since been remediated, they should be documented in the system's POA&M for tracking purposes.

6a(4). Remediation actions do not sufficiently address weaknesses (NIST SP 800-53, Rev. 3, Sect. 3.4 Monitoring Security Controls).

No

6a(5). Initial date of security weaknesses are not tracked (OMB M-04-25).

No

6a(6). Security weaknesses are not appropriately prioritized (OMB M-04-25).

No

6a(7). Estimated remediation dates are not reasonable (OMB M-04-25).

Yes

Comments: The POA&Ms for nine OPM systems contain security weaknesses with remediation activities over 120 days overdue. In the third quarter of 2010, OPM systems had a total of 58 POA&M items over 120 days overdue, an increase from 26 overdue items during the same time period in FY 2009.

This indicates that the OCIO has not provided adequate leadership and guidance to ensure that program offices assign reasonable POA&M due dates and stay on track to meet those dates. Program offices are equally responsible for dedicating adequate resources to addressing POA&M weaknesses and meeting target objectives.

6a(8). Initial target remediation dates are frequently missed (OMB M-04-25).

Section 5: Status of Plans of Actions & Milestones (POA&M) Program

Yes

Comments: See comments in 6a(7)

6a(9). POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).

No

6a(10). Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 & OMB M-04-25).

No

6a(11). Agency CIO does not track and review POA&Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).

Yes

Comments: The OIG selected one closed POA&M item from nine OPM systems and reviewed the proof of closure documentation provided by the program offices when the POA&M items were closed. Adequate proof of closure was provided for eight of the nine systems tested. Proof of closure was not available for three POA&M items selected for the ninth system, and the program office subsequently reopened these security weaknesses. The OCIO's failure to adequately review proof of closure documentation before allowing program offices to close POA&M items increases the risk that security weaknesses remain unaddressed.

6a(12). Other

No

Section 6: Status of Remote Access Program

7. Selected response is:

b. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.

7a. Areas for Improvement:

7a(1). Remote access policy is not fully developed.

Yes

Comments: Although OPM has implemented a telecommuting policy that provides guidance on the establishment, management, and maintenance of telecommuting, it does not address the technical elements of telecommuting suggested by the NIST "Guide to Enterprise Telework and Remote Access Security." In addition, the telecommuting policy has not been updated since 2001.

7a(2). Remote access procedures are not fully developed, sufficiently detailed or consistently implemented.

Section 6: Status of Remote Access Program

Yes

Comments: See comments in 7a(1).

7a(3). **Telecommuting policy is not fully developed (NIST 800-46, Section 5.1).**

Yes

Comments: See comments in 7a(1).

7a(4). **Telecommuting procedures are not fully developed or sufficiently detailed (NIST 800-46, Section 5.4).**

Yes

Comments: See comments in 7a(1).

7a(5). **Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, Section 5.1).**

No

7a(6). **Multi-factor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).**

Yes

Comments: OPM utilizes a Virtual Private Network (VPN) client to provide remote users with secure access to the agency's network environment. The OPM VPN requires username and password authentication to uniquely identify users. 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.

In FY 2009, OPM [redacted]

7a(7). **Agency has not identified all remote devices (NIST 800-46, Section 2.1).**

No

7a(8). **Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46, Section 3.1 and 4.2).**

No

7a(9). **Agency does not adequately monitor remote devices when connected to the agency's networks remotely (NIST 800-46, Section 3.2).**

Section 6: Status of Remote Access Program

No

7a(10). Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).

No

7a(11). Remote access rules of behavior are not adequate (NIST 800-53, PL-4).

No

7a(12). Remote access user agreements are not adequate (NIST 800-46, Section 5.1, NIST 800-53, PS-6).

No

7a(13). Other

No

Section 7: Status of Account and Identity Management Program

8. Selected response is:

b. The Agency has established and is maintaining an account and identity management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.

8a. Areas for Improvement:

8a(1). Account management policy is not fully developed.

No

Comments:	OPM maintains two policies regarding management of user accounts: one related to Windows network (LAN) users and the other related to mainframe users. Both policies contain procedures for creating user accounts with the appropriate level of access as well as procedures for removing access for terminated employees.

8a(2). Account management procedures are not fully developed, sufficiently detailed or consistently implemented.

No

8a(3). Active Directory is not properly implemented (NIST 800-53, AC-2).

No

8a(4). Other Non-Microsoft account management software is not properly implemented(NIST 800-53, AC-2).

No

8a(5). Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).

Section 7: Status of Account and Identity Management Program

No

8a(6). Accounts are not properly issued to new users (NIST 800-53, AC-2).

No

8a(7). Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).

No

8a(8). Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).

Yes

Comments: See comments in 7a(6).

8a(9). Agency has not adequately planned for implementation of PIV for logical access (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01).

No

8a(10). Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, AC-6).

No

8a(11). Agency does not use dual accounts for administrators (NIST 800-53, AC-5, AC-6).

No

8a(12). Network devices are not properly authenticated (NIST 800-53, IA-3).

Yes

Comments: [redacted]

8a(13). Other

No

Section 8: Status of Continuous Monitoring Program

9. Selected response is:

b. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.

9a. Areas for Improvement:

Section 8: Status of Continuous Monitoring Program

9a(1). **Continuous monitoring policy is not fully developed.**

Yes

Comments: OPM's IT Security and Privacy Policy Volume 2 states that the security controls of all systems must be tested at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and meeting the security requirements for the system.

In addition to the annual tests, OPM's infrastructure systems (LAN/WAN and Enterprise Server) are subject to additional security control tests in the form of automated vulnerability scans. Although these scans are performed routinely, the OCIO has not developed a Continuous Monitoring Policy to provide guidance on identifying high-risk security controls along with a strategy for testing them on a continuous basis.

9a(2). **Continuous monitoring procedures are not fully developed or consistently implemented.**

Yes

Comments: See comments in 9a(1).

9a(3). **Strategy or plan has not been fully developed for entity-wide continuous monitoring (NIST 800-37).**

Yes

Comments: See comments in 9a(1).

9a(4). **Ongoing assessments of selected security controls (system-specific, hybrid, and common) have not been performed (NIST 800-53, NIST 800-53A).**

Yes

Comments: The security controls were tested for only 28 of OPM's 43 systems in FY 2010

9a(5). **The following were not provided to the system authorizing official or other key system officials: security status reports covering continuous monitoring results, updates to security plans, security assessment reports, and POA&Ms (NIST 800-53, NIST 800-53A).**

No

9a(6). **Other**

Yes

Explanation for Other

List of Common Security Controls

Section 8: Status of Continuous Monitoring Program

Comments: Many of the applications in OPM's system inventory are housed in OPM's LAN/WAN or Enterprise Server (mainframe) general support systems (GSS). These applications inherit a significant portion of information security controls required by NIST SP 800-53 from these environments. These inherited controls are referred to as "common controls."

When the security controls of a system are subject to testing, the program office conducting the test is not required to evaluate the controls inherited from the GSS, as these controls are certified by OPM's OCIO. However, the OCIO does not currently maintain a published list of common security controls, and individual program offices are responsible for determining which controls are inherited from a GSS, increasing the risk that certain security controls remain untested.

Section 9: Status of Contingency Planning Program

10. Selected response is:

b. The Agency has established and is maintaining an entity-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.

10a. Areas for Improvement:

10a(1). Contingency planning policy is not fully developed.

Yes

Comments: OPM's Information Security and Privacy Policy Volume 2 states that each system owner must "Test the contingency plan for the information system at least annually to determine the plan's effectiveness and the system's readiness to execute the plan." However, this policy does not provide instructions for conducting business impact assessments, developing contingency plans, or conducting the contingency plan test in accordance with NIST guidance.

10a(2). Contingency planning procedures are not fully developed or consistently implemented.

Yes

Comments: See comments in 10a(1).

10a(3). An overall business impact assessment has not been performed (NIST SP 800-34).

No

10a(4). Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).

Section 9: Status of Contingency Planning Program

No

10a(5). A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34).

No

10a(6). A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34).

No

10a(7). System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

Comments: Up-to-date contingency plans did not exist for 7 of the 43 systems on OPM's master system inventory. Five of 43 systems had documented contingency plans, but they were not reviewed or updated in FY 2010. The OIG was not provided with evidence that a documented contingency plan exists for the remaining two systems.

10a(8). Critical systems contingency plans are not tested (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

Comments: The contingency plans for 30 of OPM's 43 systems were tested in FY 2010 in full compliance with the requirements of NIST SP 800-34, Contingency Planning Guide for Information Technology Systems. Eleven of 43 system contingency plans were tested in FY 2010, but not with a scenario-based contingency plan test conducted in accordance with NIST SP 800-34 requirements. The remaining two system contingency plans were not subject to any form of contingency plan test in FY 2010.

10a(9). Training, testing, and exercises approaches have not been developed (FCD1, NIST SP 800-34,NIST 800-53).

Yes

Comments: OPM's Information Security and Privacy Policy Volume 2 states that each system owner must "Test the contingency plan for the information system at least annually to determine the plan's effectiveness and the system's readiness to execute the plan." However, this policy does not provide instructions for conducting business impact assessments, developing contingency plans, or conducting the contingency plan test in accordance with NIST guidance.

10a(10). Training, testing, and exercises approaches have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).

No

10a(11). Disaster recovery exercises were not successful revealed significant weaknesses in the contigency planning. (NIST SP 800-34).

Section 9: Status of Contingency Planning Program

No

10a(12). After-action plans did not address issues identified during disaster recovery exercises (FCD1, NIST SP 800-34).

No

10a(13). Critical systems do not have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).

No

10a(14). Alternate processing sites are subject to same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).

No

10a(15). Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).

No

10a(16). Backups are not appropriately tested (FCD1, NIST SP 800-34, NIST SP 800-53).

No

10a(17). Backups are not properly secured and protected (FCD1, NIST SP 800-34, NIST SP 800-53).

No

10a(18). Other

No

Section 10: Status of Agency Program to Oversee Contractor Systems

11. Selected response is:

c. The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities.

Comments:

OPM's master system inventory indicates that 11 of the agency's 43 major applications are operated by a contractor.

In prior audits, OIG has verified that the security controls of these contractor systems were tested by an OPM employee. However, in FY 2010, 7 of the 11 contractor systems were not subject to security control testing.

In addition OPM does not have a formal policy providing the OCIO and other program offices guidance on the appropriate oversight of contractors and contractor-run systems.