US OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
. OFFICE OF AUDITS

Final Audit Report

Subject:

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT FY 2008

Report No. <u>4A-CI-00-08-022</u>

Date: <u>September 23. 2008</u>

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administration of the audited contract. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905); therefore, while this audit report is available under the Freedom of Information Act, caution needs to be exercised before releasing the report to the general public.

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 2008

WASHINGTON, D.C.

Report No. 4A-CI-00-08-022

Date: September 23, 2008

Michael R. Esser
Assistant Inspector General
for Audits

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT
FY 2008

WASHINGTON, D.C.

Report No. 4A-CI-00-08-022

Date: September 23, 2008

This final audit report documents the Office of Personnel Management's (OPM's) continued efforts to manage and secure its information resources. We believe that overall OPM has made progress in strengthening its information technology (IT) security program since the advent of the FISMA auditing and reporting requirements in 2002. However, we have significant concerns this year with respect to several aspects of the program.

The summary of our audit results below indicates that there are opportunities for improvement in a multitude of processes relevant to the overall IT security program at OPM, with the most notable deficiencies being related to the processes of certification and accreditation (C&A), plan of action and milestones, and maintenance of IT security policies and procedures. Specifically, the Office of the Inspector General (OIG) noted that:

- An active C&A exists for 39 of OPM's 40 systems. One system has not had an updated C&A since 2003. Another system went into production with a major element missing from its C&A package. The OIG considers this a significant deficiency in the control structure of OPM's IT security program.
- OPM has implemented an agency-wide plan of action and milestones (POA&M) process to help track and prioritize known IT security weaknesses associated with the Agency's information systems. However, the POA&M process could be improved.

- OPM's IT security policies have not been updated in at least three years. The OIG considers this condition to be a material weakness in the internal control structure of OPM's IT security program.

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

- The contingency plans for 39 out of OPM's 40 systems were tested during fiscal year (FY) 2008.
- The security controls for all40 systems in OPM's inventory were tested during FY 2008.
- OPM performs routine oversight and evaluation of its major applications operated by a contractor. However, OPM does not update its system inventory to clearly identify the state of the system (active, suspended, development, etc.).
- OPM maintains an inventory of all applications/systems under its control.
- OPM has established a process for conducting privacy impact assessments (PIAs). As of August 2008, PIAs have been completed for each of the required 28 systems.
- OPM has made good progress in implementing the requirements of the Office of Management and Budget's Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information".
- A technical configuration guide has been implemented to provide guidance for securing a variety of operating platforms in use at OPM. OPM's systems almost always adhere to the requirements of the configuration guide.
- OPM has not implemented all elements of the Federal Desktop Core Configuration requirements.
- OPM has created an "Incident Response and Reporting Policy" that describes the responsibilities of OPM's Computer Incident Response Team, and documents procedures for reporting all abnormal IT security events to the appropriate entities.
- OPM has implemented a process to provide annual and mandatory information technology security and privacy awareness training.
- The security and privacy awareness training contains a section that defines peer-to-peer file sharing, and explicitly prohibits its use on OPM networks and workstations.
- E-authentication risk assessments have been completed for the appropriate systems at OPM.

Contents

Introduction

On December 17, 2002, the President signed into law the E-Government Act (Public Law 107-347), which includes Title III, the Federal Information Security Management Act (FISMA). FISMA requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the Office of Management and Budget (OMB) the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In accordance with FISMA, we conducted an evaluation of OPM's security program and practices. As part of our evaluation, we reviewed OPM's FISMA compliance strategy and documented the status of its compliance efforts.

Background

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

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

To assist agencies in fulfilling their FISMA evaluation and reporting responsibilities, OMB issued memorandum M-08-21 (FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management). This memorandum provides a consistent form and format for agencies to report to OMB. It identifies a series of reporting topics that relate to specific agency responsibilities outlined in FISMA. Our evaluation and reporting strategies were designed in accordance with the above OMB guidance.

Objectives

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

- System Inventory
- Certification and Accreditation, Security Controls Testing, and Contingency Planning
- Agency Oversight of Contractor Systems and Quality of System Inventory
- Agency Plan of Action and Milestones Process
- Certification and Accreditation Process
- Agency Privacy Impact Assessment Process
- Agency Progress in Implementing OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- Configuration Management
- Incident Reporting

- Security Awareness Training
- Peer-to-Peer File Sharing
- E-authentication Risk Assessments
- Security Policies and Procedures Review and Update

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

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 through September 2008.

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

- Central Personnel Data File System (OIG Report No. 4A-WR-00-08-024)
- Employee Benefit Information System (OIG Report No. 4A-RI-00-08-023)
- USAJOBS (OIG Report No. 4A-HR-00-08-058)
- Executive Schedule C System (OIG Report No. 4A-M0-00-08-059)

In addition, the FY 2008 FISMA follow-up audit (OIG Report No. 4A-CI-00-08-061) indicated that the following OPM major applications had outstanding audit recommendations from the FY 2006 and FY 2005 FISMA reviews:

- GoLearn Learning Management Systems
- Government Financial Information System
- Actuaries Group System
- Learning Management System
- Fingerprint Transaction System
- Enterprise Human Resources Integration Data Warehouse
- Electronic Questionnaire for Investigations Processing
- PIPS Financial Interface System

While resource restrictions limited our ability to evaluate all major applications at OPM, we believe that the results of the evaluations listed above are a fair representation of OPM's overall FISMA compliance status.

We considered the internal control structure for various OPM systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls for these various systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of these systems' internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented. As appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

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

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

The criteria used in conducting this audit include:

- OPM Information Technology Security Policy;
- OPM IT Security Program Plan;
- OMB Circular A-130, Appendix Ill, Security of Federal Automated Information Resources;
- OMB Memorandum M-08-21, FY 2008 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-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems;
- 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 800-26, Self Assessment Guide for Information Technology 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 1, 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 2008 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, program offices were not in complete compliance with all standards, as described in the "Results" section of this report.

Results

The sections below detail the results of the OIG's audit of OPM's FISMA compliance efforts. The results are formatted to be consistent with the questions outlined in the FY 2008 OMB Reporting Template for IGs.

I. System Inventory

OPM has identified 40 major applications/systems within eight of its program offices. OPM's system inventory indicated that these 40 systems were comprised of the following PIPS 199 system impact classifications: 7 high, 32 moderate, and 1 low. The inventory also indicated that 30 systems operated within the agency and 10 are operated at a contractor facility.

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

a) Number of systems certified and accredited (C&A)

A C&A has been completed and remains active for 39 of the 40 systems in OPM's inventory. See section V below for details of the system without a current C&A and a review of OPM's C&A process.

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

FISMA requires each agency to perform for all systems "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually ...."

The Center for Information Services and Chief Information Officer (CIS/CIO) at OPM has implemented procedures for conducting an annual review of the security controls for each of the agency's systems. These controls are tested through either an annual self-assessment or through a security test and evaluation conducted by an independent source as part of the C&A process.

The OIG determined that as of August 2008 the security controls had been tested for 37 of OPM's 40 systems during the past year. We judgmentally selected 5 of these 37 systems and conducted a detailed review of the documentation resulting from the test of security controls. We found that the security controls tests for all five systems in the sample were completed in accordance with NIST SP 800-53 Revision I guidance. The results of this sample were not projected to the entire population.

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.

Recommendation 1

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

CIS/CIO Response:

"We concur.

In addition, we are providing [evidence that the security controls have been tested for the remaining systems]."

OIG Reply:

We acknowledge that a test of security controls was conducted for the remaining three systems. However, due to the fact that this documentation was submitted to the OIG after the draft audit report was issued, we did not have sufficient time to evaluate the quality of these tests of security controls. We will evaluate the quality of the security controls tests submitted after the fieldwork phase of this audit as part of the 2009 FISMA audit.

c) Number of systems for which contingency plans have been tested

FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis.

The OIG judgmentally selected a sample of5 out of OPM's 40 system contingency plans and conducted an in-depth review of these plans to ensure that they met the requirements of NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems." The review included, but was 'not limited to, the following elements of the contingency plan:

- System recovery on an alternate platform from backup media;
- Coordination among recovery teams;
- Internal and external connectivity;
- System performance using alternate equipment;
- Notification procedures.

Nothing came to our attention to indicate that these contingency plans were not in compliance with NIST guidance. The results of this sample were not projected to the entire population.

The OIG received documentation indicating that the contingency plans for 36 of OPM's 40 systems were tested in the past year.

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

Recommendation 2

We recommend that OPM's program offices program test the contingency plans for each system on an annual basis.

CIS/CIO Response:

"We concur.

We are providing contingency plan test results for {three of the four systems that were missing on the date the draft audit report was issued]."

OIG Reply:

The CIS/CIO's response to the draft report included evidence of four additional contingency plan tests. However, only three of these four contingency plan tests correspond to the four that were identified as missing as of the date the draft audit report was issued. Therefore, one system continues to lack a contingency plan test less than one year old. We continue to recommend the contingency plans for a1140 OPM systems be tested on an annual basis.

III. Agency Oversight of Contractor Systems and Quality of System Inventory

The CIS/CIO continuously maintains a master inventory of OPM's major systems. The CIS/CIO relies on the various program offices to identify the existence and status of systems to be included in the inventory. The OIG agrees with the total number of systems listed in the most recent system inventory (40) and agrees with the number of systems operated by a contractor (10).

OPM performs routine oversight and evaluation of its systems operated by a contractor. Each of the 10 OPM systems that are operated by a contractor have been certified and accredited by OPM. In addition, the annual self-assessment of IT security controls for each of these systems was conducted by an OPM employee.

Although OPM's system inventory accurately identifies all of the agency's active major systems, it also lists systems that are still in development and have not been certified and accredited. These systems are not clearly labeled as inactive or in development, which could lead to an inaccurate count of the total number of systems.

Recommendation 3

We recommend that OPM update its system inventory to clearly identify the state of the system (active, suspended, development, etc.).

<u>CIS/CIO Response:</u>

"We concur."

IV. Agency Plan of Action and Milestones Process

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

a) The POA&M is an agency-wide process, incorporating all known IT security weaknesses

OPM has implemented an agency-wide POA&M process to help track known IT security weaknesses associated with the agency's information systems. However, we found that three POA&Ms did not contain all security weaknesses identified during security controls tests of those systems.

Failure to include all security weaknesses on POA&Ms limits the CIS/CIO's ability to monitor the program office's efforts in correcting IT security weaknesses.

<u>Recommendation 4</u>

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

<u>CIS/CIO Response:</u>

"We concur."

b) Program officials develop, implement, and manage POA&Ms for their systems

OPM program office officials are responsible for developing, implementing, and managing POA&M's for each system that they own and operate. The OIG was provided evidence that POA&Ms are continuously managed for only 38 of OPM's 40 systems.

<u>Recommendation 5</u>

We recommend that an up-to-date POA&M exist for each system in OPM's inventory.

<u>CIS/CIO Response:</u>

"We concur.

In addition, we are the providing two system POA&Ms that we had not previously submitted as part of the original audit request."

OIG Reply:

We acknowledge that a current POA&M exists and has been routinely updated for one of the two systems in question. However, the POA&M for the [redacted] system provided to the OIG in response to the draft audit report was created on August 25, 2008, and had not been managed or updated since February 2007. Furthermore, this POA&M did not incorporate the majority of the security vulnerabilities identified during the 2008 security controls testing for [redacted] The OIG believes that this represents a weakness in OPM's overall POA&M process, and continues to recommend that POA&M be continuously managed for each system in OPM's inventory.

c) Program officials and contractors report their progress on security weakness remediation to the CIO

On a quarterly basis, OPM program officials are required to send the CIS/CIO an updated POA&M detailing the progress made in correcting the system's security weaknesses. However, POA&Ms were not submitted to the CIS/CIO for 3 systems in the third quarter of 2008.

Recommendation 6

We recommend that all program offices submit POA&Ms to the CIS/CIO office on a quarterly basis.

CIS/CIO Response:
"We concur.

We are providing a total of three system POA&Ms that had not been previously submitted as a part of the original audit request. Two of these POA&Ms were provided as part of Recommendation 5. The third POA&M was not provided because it was a negative report, therefore no weaknesses were identified to report for that system. In the future, we will request that all systems provide a quarterly POA&M whether or not weaknesses are identified for each system."

OIG Reply:

The POA&MS provided by CIS/CIO in response to the draft audit report were for the 4th Quarter of 2008. This audit recommendation resulted from tests of 3rd quarter POA&M submissions which showed that POA&Ms for 3 of OPM's 40 systems were missing. We continue to recommend that all program offices submit POA&Ms to the CIS/CIO on a quarterly basis.

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

OPM's agency-wide POA&M process requires program offices to provide the CIS/CIO with evidence, or "proof of closure," that the weaknesses identified in POA&Ms have been resolved.

The OIG judgmentally selected POA&M items from 13 systems and asked the CIS/CIO to provide the proof of closure documentation that they had received from the program offices when the POA&M item was labeled as "complete." The CIS/CIO was able to provide proof of closure documentation for only 6 of these 13 systems[1].

Recommendation 7

We recommend that the CIS/CIO require each program office to provide evidence (proof of closure) that POA&M weaknesses have been resolved before allowing that item to be labeled "complete."

CIS/CIO Response:

"We concur."

e) IG findings are incorporated into the POA&M process

In FY 2007, the OIG conducted audits of four OPM systems, and verified that the recommendations from these four audit reports were incorporated into the respective system's POA&M. However, three privacy program related audit recommendations from the OIG's 2007 FISMA final audit report did not appear on the POA&M maintained by OPM's Plans and Policies Group.

In addition, OIG audit recommendations for one OPM system appeared on an older version of the POA&Ms for that system, but were not included in the most recent version.

Recommendation 8

We recommend that all OIG recommendations be included on POA&Ms and they not be removed until evidence of proof of closure is provided to the CIS/CIO.

CIS/CIO Response:

"We concur."

f) POA&M process prioritizes IT security weaknesses

Each program office at OPM prioritizes IT security weaknesses on their POA&Ms to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.

[1] In the OMB FISMA Reporting Template for Inspectors General, Question 4 (see Appendix A), we projected these results across the entire system population (40). Consequently, we determined that 46% of the systems POA&M activities are tracked by the CIS/CIO.

V. Certification and Accreditation Process

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

The OIG reviewed the C&A documentation for all OPM systems in which a C&A was due in FY 2008. During this review we discovered that one system was operating with an expired C&A, and another (new) system went into a live operating status without a complete C&A package. It is the responsibility of OPM's CIS/CIO to ensure that all live/production systems in OPM's inventory are subject to a complete C&A every three years, as required by FISMA. We believe that the following weaknesses in OPM's C&A process indicate a significant deficiency in the control structure of OPM's IT security program:

a) Expired C&A

OPM's [redacted] system has not been subject to a full C&A since 2003. The system did go through a partial C&A in 2006, but the process did not include an independent test of the system's security controls. The 2006 C&A documentation included an extended authorization to operate (ATO) for one year, as a new system was scheduled to replace [redacted] in January 2007. In 2007, the ATO was extended for an additional year because the release date of the new system was pushed back to August 2007.

As of August 2008, the ATO for [redacted] has been extended a third time with no specified expiration date.

Recommendation 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.

CIS/CIO Response:

"We concur.

In addition, we are providing the C&A for [redacted]

OIG Reply:

The documentation provided to the OIG in response to recommendation 9 included a fourth extension to the [redacted] system's ATO, and did not comprise a complete C&A package as required by FISMA. Specifically, the 2008 C&A documentation for [redacted]

- Did not contain a current Information System Security Plan (ISSP). The ISSP provided was developed in August 2003.
- Did not contain a contingency plan.

- Did not contain a current contingency plan test.
- Did not contain signed Certification and Accreditation statements.
- Contained an incomplete POA&M; the POA&M provided did not include all of the vulnerabilities identified in the August 25, 2008 Baseline Security Requirements Test for [redacted]

The OIG continues to consider the fact that [redacted] has not been fully C&A'd in over five years a significant deficiency in the control structure of OPM's IT security program.

b) Missing element from C&A

The OIG conducted a detailed review of the C&A packages that were completed during the past year. While the majority of the system's C&A documentation contained all of the elements required by FISMA and relevant NIST guidance, the C&A statements for one system were signed and approved even though a business contingency plan had not been created for that system. Although the OIG acknowledges that the missing contingency plan is listed as an action item on that system's POA&M, we believe that a system should not be C&A'd and allowed to go into a live/production status without a contingency plan in place.

Recommendation 10

We recommend that all elements required by FISMA and relevant NIST guidance be in place before a system is formally C&A'd.

CIS/CIO Response:

"We concur. However, business reasons may compel the issuance of an JATO without all the required elements of a C&Apackage in place. As such, required components not included in the C&A package will be added to the appropriate system POA&M as weaknesses to be completed in a timely manner."

OIG Reply:

We acknowledge that business reasons may compel the issuance of an *interim* ATO (IATO) without all the required elements of a C&A package in place. When taking this approach, the IATO should be set to expire after a period of time sufficient to remedy the outstanding problems (which should be no more than several months), at which point a full ATO can be issued. However, the system with a missing contingency plan received a full C&A with a three-year ATO signed by the Associate Director of the program office that owns the system.

VI. Agency Privacy Impact Assessment Process

The £-Government Act of 2002, section 208, requires agencies to conduct privacy impact assessments (PIA) of information systems that process personally identifiable information (PII). In 2007, OPM's IT security officer issued a "PII Questionnaire" to the designated security officer for each of the Agency's major systems to determine whether the system contains PII. The results of the questionnaire indicated that 37 of OPM's 40 systems contained at least some PII. Of these 37 systems, 28 require PIAs.

OPM's PIA Guide states that the Agency's Plan and Policies Group (PPG) is responsible for obtaining the CIO's review of the initial screening and PIA, if required. PPG is also responsible for publishing the PIA on OPM's website and sending a copy to OMB. As of August 2008, summaries of all 28 required PIAs had been published to OPM's website. OPM intends to replace each PIA summary with a full PIA prior to September 30, 2008.

VII. Agency Progress in Implementing OMB M-07-16

The OIG evaluated OPM's privacy program by conducting a qualitative assessment of the agency's progress in implementing OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." OMB M-07-16 requires all federal agencies to develop and implement a "breach notification policy." The memorandum provides a framework for creating the policy, and outlines security and privacy requirements related to the protection of PII. The sections below highlight OPM's progress in implementing the various requirements ofM-07-16.

a) Implement a breach notification policy

OPM has developed an "Information and Security and Privacy Policy" that contains breach notification procedures. The policy identifies the internal and external entities that must be notified when a security breach occurs. OPM's Director also issued an agency-wide email labeled "New Procedures Regarding the Use of Personally Identifiable Information." This message provided OPM employees with specific instructions to notify the agency's "situation room" immediately after detecting any security or privacy breach.

Although the Information Security and Privacy policy has received final approval from OPM's senior management, it has not been distributed to the agency's general population of information system users.

Recommendation 11

We recommend that OPM issue its "Information Security and Privacy Policy" to all agency employees and post a copy to the agency's internal website.

CIS/CIO Response:

"We concur. The document has been posted on {OPM 's internal website]."

OIG Reply:

No further action is required.

b) Privacy requirements

OMB M-07-16 requires agencies to review and reduce the volume of PII processed through its systems.

Review Current Holdings

As mentioned in the Privacy Impact Assessment section above, each of OPM's program offices completed a "PII Questionnaire" to evaluate the current holdings of PII on the information systems they own.

OPM's PIA Guide also mentions that it is the responsibility of each program office to review and update their PIAs on an annual basis.

Reduce the Use o[Social Security Numbers

OMB M-07-16 requires agencies to establish a plan to eliminate the unnecessary collection and use of social security numbers (SSNs) within 18 months. OPM has taken several steps to reduce the use of SSNs in its systems and programs, including:

- OPM's Director issued a memo to all Chief Human Capital Officers providing guidance to agencies to protect and eliminate the unnecessary use of SSNs.
- The designated security officers of OPM's major systems have been briefed on their responsibility for evaluating the unnecessary use of SSNs on their respective systems.
- OPM has participated in the Interagency Best Practices Collaborative meeting to discuss ways of eliminating unnecessary SSNs and to share information on the development of an alternative identifier.
- OPM has a "Forms Officer" designated with the responsibility of reviewing OPM-owned forms to ensure the reduction or elimination of unnecessary use of SSNs.

Recommendation 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.

CIS/CIO Response:

"We concur with the thrust of the recommendation and will continue our efforts to reduce the use of SSNs and will update our formal plan to eliminate the unnecessary collection and use of SSNs."

c) Security requirements

The security requirements outlined in OMB M-07-16 reference the elements below that originated from a prior OMB Memorandum, "Protection of Sensitive Agency Information" (M-06-16).

Encryption

OPM's IT Security and Privacy Policy requires that all sensitive data on mobile computers be encrypted with FIPS 140-2 validated cryptographic modules. The agency has implemented a temporary solution that requires users to manually encrypt sensitive data using WinZip. OPM is in the process of developing a solution to automatically encrypt sensitive data on mobile computers.

Recommendation 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.

CIS/CIO Response:

"We concur."

Control Remote Access

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

Time Out Function

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

Log and Verify

OPM does not currently have an agency-wide methodology for logging computer-readable data extracts and is unable to determine whether sensitive data has been erased after 90 days.

Recommendation 14

We recommend that OPM continue its efforts to develop a methodology for logging computer-readable data extracts to determine whether sensitive data has been erased after 90 days.

CIS/CIO Response:

"We concur with the need to continue the efforts to develop a methodology f or logging computer-readable data extracts."

d) Incident reporting and handling requirements

See section IX. "Incident Reporting"

e) Rules and consequences

In addition to the "Information Security and Privacy Policy" and the "New Procedures Regarding the Use of Personally Identifiable Information," OPM has issued several additional policies and guidance related to rules and responsibilities regarding the protection of PII, including:

- OPM Guidelines for Handling PII- outlines specific rules to follow while possessing PII outside of a secure worksite.
- Security, Privacy, and 508 Contract Compliance Requirements- sets forth requirements for contractors that have access to PII.
- Situation Room Incident Response Procedures - provides detailed procedures to be followed by the situation room when they are notified of a PII breach.

Although OPM's "Information Security and Privacy Policy" outlines corrective actions that can be imposed for the failure to adequately protect PII, this policy is not currently available to all OPM system users. However, the agency has conducted mandatory online "PII Responsibilities" training that stated that the corrective actions for improper disclosure of PII may range from counseling to removal, and that additional penalties covered in the Privacy Act could also be implemented.

VIII. Configuration Management

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

a) Agency-wide security configuration policy

FISMA requires each agency to develop minimally acceptable system configuration requirements for all operating platforms in use at that agency. OPM's Network Management Group (NMG) has implemented configuration guides for securing its [redacted] operating platforms. Furthermore, OPM's OIG has implemented configuration guides for securing [redacted], and the Application Systems Group (ASG) has implemented a configuration policy for securing [redacted]

b) Extent to which systems implement common security configurations

NMG provided the OIG with documentation indicating that the Agency's systems adhere to the configuration guidelines for [redacted]. An independent contractor reviewed the configuration of the Agency's single [redacted] system to confirm compliance with the secure configuration guide.

The OIG conducted a vulnerability scan of 10 production [redacted] at OPM. The results of the scans indicated that all 10 [redacted] contained at least 1 configuration setting that was not compliant with OPM's [redacted] configuration policy.

Due to privacy and security concerns, the technical details of these vulnerabilities will not be included in this audit report. However, this information has been provided to OPM's CIS/CIO and ASG through an informal audit inquiry.

Recommendation 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' owner should document the reason in the system's ISSP to formally accept any associated risks.

CIS/CIO Response:

"We concur.

In addition, we have addressed the discovered vulnerabilities and provided the supporting documentation to the OIG."

OIG Reply:

The OIG agrees that OPM's ASG has addressed the discovered vulnerabilities for 5 of the 10 [redacted] that were part of this review. Each of the five additional [redacted] has a single outstanding vulnerability in common. These five [redacted] are all running [redacted] [redacted]. Because [redacted] is no longer supported by the vendor, OPM is hesitant to make the system changes necessary to address this vulnerability.

Two of the 40 systems in OPM's inventory are affected by the vulnerability in these 5 [redacted]. The owner of one of these systems has formally accepted the risks associated with operating an outdated version of [redacted] If ASG does not wish to update the other [redacted], we recommend that ASG work with the CIS/CIO to notify the system owners of the vulnerability so that the system owner can incorporate an acceptance of the vulnerability risk into their ISSP.

c) Federal desktop core configuration

OMB Memorandum M-07-11 required Federal agencies to implement standard security configurations for [redacted] by February 2008. These standard configurations were developed by NIST, the Department of Defense, and the Department of Homeland Security, and became known as the Federal Desktop Core Configuration (FDCC).

As of August 2008, OPM has created a new standard [redacted] image that generally adheres to FDCC requirements, and settings that deviate from FDCC requirements have been documented. However, the FDCC settings have only been implemented in one program office at OPM. Furthermore, OPM has not included New Federal Acquisition Regulation 2007-004language into all contracts related to common security settings.

Recommendation 16

We recommend that OPM continue its efforts to implement all required elements of the FDCC.

CIS/CIO Response:

"We concur."

IX. Incident Reporting

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

a) Identifying and reporting incidents internally

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

OPM also notifies the OIG when security incidents occur by providing OIG investigators with a monthly report that tracks the security tickets related with the loss of sensitive data. In addition, an OIG representative was added to OPM's incident notification email distribution list.

b) Reporting incidents to US-CERT

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

c) Reporting incidents to law enforcement

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

X. Security Awareness Training

The CIS/CIO at OPM has implemented a process to provide annual IT security and privacy awareness training. OPM's IT Security Policy states that "Education and training are key elements in our IT Security Program. At a minimum, annual computer security awareness training is mandatory for all OPM users."

The training is conducted through an interactive online course provided through OPM's online training website. The course introduces employees and contractors to the basic concepts of IT security and privacy. The comprehensive training covers various topics such as: the importance of information security; threats and vulnerabilities; viruses and malicious codes; privacy training; and roles and responsibilities of users. Individuals are required to complete an assessment at the end of the training course to verify their understanding of the material.

In FY 2008, the CIS/CIO implemented various controls to ensure that the training was completed as required. Such controls include, but are not limited to, notifying various levels of management of individuals who had not completed the training and temporarily disabling system access to those who have not completed the training in a timely manner.

The CIS/CIO's goal was to have all employees and contractors complete the training by July 25,2008. As of September 2008, over 96 percent of the 12,231 OPM employees and contractors have completed the training.

Recommendation 17

We recommend that OPM continue its efforts to ensure that all federal employees and contractors with access to OPM's IT resources complete IT security and privacy awareness training on an annual basis.

CIS/CIO Response:

We concur. We are providing screenshots of our current status for the Security Awareness Training completion percentage from the GoLearn portal. Our current agency wide completion rate for Security Awareness Training is 98.32%.

XI. Peer-to-Peer File Sharing

FISMA requires agencies to implement policies regarding the use of peer-to-peer file sharing on its networks. Peer-to-peer software programs traditionally bypass network security controls. All OPM employees and contractors are required to take an online IT security and privacy awareness training course (see section X. Security Awareness Training). The annual training course contains a section that defines peer-to-peer file sharing and explicitly prohibits its use on OPM networks and workstations.

XII. E-authentication Risk Assessments

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

M-04-04 requires agencies to identify the various electronic transactions conducted by each system and ensure that authentication processes provide the appropriate level of assurance. The guidance identifies four levels of identity assurance for electronic transactions, and outlines a five step process to determine the appropriate assurance level of each transaction.

According to OPM's official system inventory, seven of the Agency's systems are subject to e-authentication requirements. The OIG was provided withe-authentication risk assessments for six of these seven systems.

Recommendation 18

We recommend that e-authentication risk assessments be completed for the required systems in accordance with OMB M-04-04.

CIS/CIO Response:

We concur. We are providing thee-authentication risk assessment for eOPF to the OIG.

OIG Reply:

No further action is required.

XIII. Security Policies and Procedures Review and Update

The CIS/CIO follows the issuance of new IT security guidance closely and provides applicable guidance to agency DSOs in a timely manner. However, this information has not been routinely incorporated into the Agency's IT security policies.

As indicated in the table below, the majority of OPM's IT security polices and procedures available to OPM employees via the agency's intranet (THEO) have not been updated in at least three years.

IT Security Policies on OPM Intranet (THEO)	Issue Date (Per THEO)
IT Security Program Plan	May 2003
IT Security Program Plan Implementation Guide	May2003
IT Security Policy Implementation Guide - Certification and Accreditation	May2003

IT Security Policy Implementation Guide - Security Documentation Requirements	April 2003
IT Security Policy Implementation Guide - Incident Response and Reporting policy	July 2005

OPM did provide the OIG with an updated "IT Security Policy Implementation Guide - Incident Response and Reporting." However, this policy has not been updated on THEO. As a result, OPM employees do not have access to the most recent OPM policy on reporting data breaches.

OPM's failure to adequately update IT security policies and procedures has been highlighted in the past three OIG FISMA audit reports. We acknowledge the steps that OPM has taken in creating updated policies and procedures, but will continue to consider this condition a material weakness in OPM's IT security program until all policies and procedures have been updated and published to THEO.

Recommendation 19

We recommend that the CIS/CIO promptly update OPM's IT security policies and publish them to THEO.

CIS/CIO Response:

"We concur that the CIS/CIO promptly update OPM's IT security policies and publish them to THEO. However, we disagree with the determination that this a material weakness."

OIG Reply:

This recommendation was first identified as a material weakness in the FY 2007 FISMA audit report, in which the CIS/CIO concurred with our position. IT security policies and procedures are the foundation of an IT security program. Without reasonably current policies and procedures, the program will be ineffective. In FY 2008, the majority of these policies have gone another year without a documented update, and the OIG continues to believe that this condition represents a material weakness in OPM's IT security program.

Additional CIS/C/O Comments on Excerpts from Draft Audit Report:

Draft Report Excerpt 1:

"OPM did provide the OIG with an updated "IT Security Policy Implementation Guide Incident Response and Reporting." However, this policy has not been updated on THEO. As a result, OPM employees do not have access to the most recent OPM policy on reporting data breaches."

<u>CIS/CIO Comment:</u>

"We disagree with this comment. "IT Security Policy Implementation Guide Incident Response and Reporting" that is posted on THEO is current."

OIG Reply:

We continue to believe that the copy of the IT Security Policy Implementation Guide - Incident Response and Reporting available to OPM employees via THEO is not the most current copy of the document. The copy provided to the OIG during the FY 2008 FISMA audit indicates a review/revision was completed in March/April 2008. However, the copy available on THEO indicates that the last review/revision was in July 2005.

Draft Report Excerpt 2:

"We acknowledge the steps that OPM has taken in creating updated policies and procedures, but will continue to consider this condition a material weakness in OPM's IT security program until all policies and procedures have been updated and published to THEO."

<u>CIS/CIO Comment:</u>

"The agency's Information Security and Privacy Policy have been published to THEO. In addition, the remainder of the documents cited were reviewed during February 2008 as part of an ongoing review of OPM's information security and privacy policy. We determined that the policies and procedures substantively represent current policies and practices and no immediate changes were deemed to be required. Furthermore, we are scheduling another review of these policies and procedures to ensure alignment in FY09. Based on the information provided above we do not believe this weakness could be considered material."

OIG Reply:

The OIG has not received any evidence that the documents cited were reviewed in February 2008, and the revision history in each of the documents on THEO also provides no indication that this review took place. The list below provides specific evidence that the IT security policies and procedures are in urgent need of update, and that they have not been subject to recent reviews as suggested by the CIS/CIO. The multitude of outdated, inaccurate, or irrelevant material contained within these policies and procedures leads the OIG to continue to assert that this represents a material weakness in OPM's IT Security Program.

Weaknesses in OPM IT security policies and procedures contained on THEO *(Note- this list may not represent all deficiencies in OPM's IT security policies and procedures, and should not be used as a "checklist" to resolve this audit recommendation):*

- OPM's IT Security Program Plan references OPM's IT Security Policy, which no longer exists as it has been replaced by the IT Security and Privacy Policy.
- OPM's IT Security Program Plan provides contact information for an ITSO who has not worked at OPM for several years.
- OPM's IT Security Program Plan references outdated NIST guidance (Special Publications that have been replaced by subsequent revisions).

- OPM's IT Security Program Plan Implementation Guide references outdated NIST guidance (Special Publications that have been replaced by subsequent revisions).
- OPM's IT Security Program Plan Implementation Guide states that NIST SP 800-26, "Security Self-Assessment Guide for Information Technology Systems" should be used as a tool to conduct self-assessments of OPM systems. However, FISMA no longer recognizes NIST 800-26 as an acceptable tool, and requires the use of NIST SP 800-53 as a self-assessment guide.
- OPM' s IT Security Program Plan Implementation Guide outlines deadlines for quarterly POA&M submissions that are no longer accurate.
- OPM's IT Security Program Plan Implementation Guide outlines deadlines for self-assessment submissions that are no longer enforced.
- OPM's IT Security Program Plan Implementation Guide provides contact information for an ITSO who has not worked at OPM for several years.
- OPM's IT Security Program Plan Implementation Guide includes a POA&M template that is outdated. OPM's current POA&M template has been modified to include a column to prioritize POA&M weaknesses.
- OPM's IT Security Policy Implementation Guide- Certification and Accreditation does not identify a POA&M, contingency plan, or contingency plan test as required documentation to be submitted with a C&A package.
- OPM's IT Security Policy Implementation Guide- Incident Response and Reporting indicates that OPM employees should contact the OPM Help Desk to report security incidents. However, new procedures issued by the Director indicate that the OPM Situation Room should be notified of security/privacy incidents.
- OPM's IT Security Policy Implementation Guide- Incident Response and Reporting contains the contact information of at least five individuals who are no longer employed at OPM.
- OPM's IT Security Policy Implementation Guide- Security Documentation Requirements does not indicate that a POA&M is required to be in place prior to authorizing a system for processing, as required by FISMA.
- OPM's IT Security Policy Implementation Guide- Security Documentation Requirements references OPM's IT Security policy, which no longer exists as it has been replaced by the IT Security and Privacy Policy.

Major Contributors to this Report

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

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

Appendix A

OFFICE OF MANAGEMENT AND BUDGET FISMA REPORTING TEMPLATE FOR INSPECTORS GENERAL

Sectio[illegible] - Inspector General: Questions 1 and 2

Agency Name:	**Office of Personnel Management**	**Submission date:**	**Sept. 23, 2008**

Question 1: FISMA Systems Inventory

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

2. For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems (Agency and Contractor systems)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Bureau Name	**FIPS 199 System Impact Level**	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Component/Bureau	High	5	5	2	2	7	7	7	100%	7	100%	7	100%
	Moderate	24	24	8	8	32	32	31	97%	32	100%	31	97%
	Low	1	1	0	0	1	1	1	100%	1	100%	1	100%
	Not Categorized					0	0						
	Sub-total	**30**	**30**	**10**	**10**	**40**	**40**	**39**	98%	**40**	100%	**39**	98%
Component/Bureau	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
Component/Bureau	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
Component/Bureau	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
Component/Bureau	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
Component/Bureau	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
Agency Totals	**High**	**5**	**5**	**2**	**2**	**7**	**7**	**7**	100%	**7**	100%	**7**	100%
	Moderate	**24**	**24**	**8**	**8**	**32**	**32**	**31**	97%	**32**	100%	**31**	97%
	Low	**1**	**1**	**0**	**0**	**1**	**1**	**1**	100%	**1**	100%	**1**	100%
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
	Total	**30**	**30**	**10**	**10**	**40**	**40**	**39**	98%	**40**	100%	**39**	98%

🟨	= Data Entry Cells
⬜	= Editable Calculations (no Data Entry-ONLY edit Formulas when necessary)

Section C - Inspector General: Question 3

Agency Name: **Office of Personnel Management**

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory

3.a.	**The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.** Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance. Response Categories: - Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	Almost Always (96-100% of the time)
3.b.	**The agency has developed a complete inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.** Response Categories: - The inventory is approximately 0-50% complete - The inventory is approximately 51-70% complete - The inventory is approximately 71-80% complete - The inventory is approximately 81-95% complete - The inventory is approximately 96-100% complete	Inventory is 96-100% complete
3.c.	**The IG generally agrees with the CIO on the number of agency-owned systems. Yes or No.**	Yes
3.d.	**The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes or No.**	Yes
3.e.	**The agency inventory is maintained and updated at least annually. Yes or No.**	Yes

3.f. **If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.**

Component/Bureau	System Name	Exhibit 53 Unique Project Identifier (UPI) {must be 23-digits}	Agency or Contractor system?

Number of known systems missing from inventory:	

🟨 = Data Entry Cells

Sectio - Inspector General: Questions 4 and 5

Agency Name:	**Office of Personnel Management**

Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process

Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.

For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.

Response Categories:

- **Rarely- for example, approximately 0-50% of the time**
- **Sometimes- for example, approximately 51-70% of the time**
- **Frequently- for example, approximately 71-80% of the time**
- **Mostly- for example, approximately 81-95% of the time**
- **Almost Always- for example, approximately 96-100% of the time**

4.a.	The POA&M is an agency-wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	Mostly (81-95% of the time)
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	Almost Always (96-100% of the time)
4.c.	Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).	Mostly (81-95% of the time)
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Rarely (0-50% of the time)
4.e.	IG findings are incorporated into the POA&M process.	Mostly (81-95% of the time)
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Almost Always (96-100% of the time)
POA&M process comments:	**The OIG considers the weaknesses in OPM's overall POA&M process a significant deficiency in the control structure of OPM's IT security program.**	

Question 5: IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate.

Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Informatic[redacted] and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.

5.a.	**The IG rates the overall quality of the Agency's certification and accreditation process as:** Response Categories: - Excellent - Good - Satisfactory - Poor - Failing		Satisfactory
5.b.	**The IG's quality rating included or considered the following aspects of the C&A process:** (check all that apply)	Security plan	X
		System impact level	X
		System test and evaluation	X
		Security control testing	X
		Incident handling	X
		Security awareness training	X
		Configurations/patching	X
		Other:	
C&A process comments:	One system has not received an updated C&A since 2003. Another system went into production with a major element missing from its C&A package. The OIG considers this a significant deficiency in the control structure of OPM's IT security program.		

Section Inspector General: Questions 6, 7, and 8

Agency Name:	**Office of Personnel Management**	
	Question 6-7: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process	
6	**Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D Question #5 (SAOP reporting template), including adherence to existing policy, guidance, and standards.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Excellent
Comments:		
7	**Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	**Good**
Comments:		
	Question 8: Configuration Management	
8.a.	**Is there an agency-wide security configuration policy? Yes or No.**	Yes
Comments:	As of the date the FISMA draft audit report was issued, 10 of 10 [redacted] reviewed by the OIG contained vulnerabilities or issues of non-compliance with the security configuration policy. The weaknesses for 9 of 10 [redacted] were corrected or the risk was formally accepted in August 2008.	
8.b.	**Approximate the extent to which applicable systems implement common security configurations, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov.** **Response categories:**	Almost Always (96-100% of the time)
	- Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	
8.c.	**Indicate which aspects of Federal Desktop Core Configuration (FDCC) have been implemented as of this report:**	
	c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations. Yes or No.	Almost Always (96-100% of the time)
	c.2 New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology", is included in all contracts related to common security settings. Yes or No.	Rarely (0-50% of the time)
	c.3 All [redacted] computing systems have implemented the FDCC security settings. Yes or No.	Rarely (0-50% of the time)

Section C: Inspector General: Questions 9, 10 and 11

Agency Name:	Office of Personnel Management

Question 9: Incident Reporting

Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.

9.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
9.b.	The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)	Yes
9.c.	The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.	Yes
Comments:		

Question 10: Security Awareness Training

Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities? Response Categories: - Rarely- or approximately 0-50% of employees - Sometimes- or approximately 51-70% of employees - Frequently- or approximately 71-80% of employees - Mostly- or approximately 81-95% of employees - Almost Always- or approximately 96-100% of employees	Almost Always (96-100% of employees)

Question 11: Collaborative Web Technologies and Peer-to-Peer File Sharing

Does the agency explain policies regarding the use of collaborative web technologies and peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes or No.	Yes

Question 12: E-Authentication Risk Assessments

12.a. Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST Special Publication 800-63, "Electronic Authentication Guidelines"? Yes or No.	Yes
12.b. If the response is "No", then please identify the systems in which the agency has not implemented the e-authentication guidance and indicate if the agency has a planned date of remediation.	

Appendix B

Center for Information Services and Chief Information Officer's September 3, 2008 response to the OIG's draft audit report, issued August 12, 2008.

Recommendation 1
We recommend that OPM ensure that an annual test of security controls has been completed for all systems.

Comments
We concur.

In addition, we are providing Paper Data Capture and Conversion Services (PDCCS) and Leadership Website annual test of security controls.

Recommendation 2
We recommend that OPM's program offices test the contingency plans for each system on an annual basis.

Comments
We concur.

We are providing contingency plan test results for the PDCCS, Enterprise Human Resources Integration (EHRI) Data Warehouse, Electronic Official Personnel Folder (eOPF), and Leadership Website systems as evidence that their contingency plans have been tested this fiscal year.

Recommendation 3
We recommend that OPM update its system inventory to clearly identify the state of the system (active, suspended, development, etc.).

Comments
We concur.

Recommendation 4
We recommend that the program offices incorporate all known security weaknesses into the POA&Ms.

Comments
We concur.

Recommendation 5
We recommend that an up-to-date POA&M exist for each system in OPM's inventory.

Comments
We concur.

In addition, we are the providing two system POA&Ms that we had not previously submitted as part of the original audit request.

Recommendation 6

We recommend that all program offices submit POA&Ms to the CIS/CIO office on a quarterly basis.

Comments

We concur.

We are providing a total of three system POA&Ms that had not been previously submitted as a part of the original audit request. Two of these POA&Ms were provided as part of Recommendation 5. The third POA&M was not provided because it was a negative report, therefore no weaknesses were identified to report for that system. In the future, we will request that all systems provide a quarterly POA&M whether or not weaknesses are identified for each system.

Recommendation 7

We recommend that the CIS/CIO require each program office to provide evidence (proof of closure) that POA&M weaknesses have been resolved before allowing that item to be labeled "complete."

Comments

We concur.

Recommendation 8

We recommend that all OIG recommendations be included on POA&Ms and they not be removed until evidence of proof of closure is provided to the CIS/CIOs office.

Comments

We concur.

Recommendation 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.

Comment

We concur.

In addition, we are providing the C&A for [redacted]

Recommendation 10

We recommend that all elements required by FISMA and relevant NIST guidance be in place before a system is formally C&A'd.

Comment
We concur. However, business reasons may compel the issuance of an IATO without all the required elements of a C&A package in place. As such, required components not included in the C&A package will be added to the appropriate system POA&M as weaknesses to be completed in a timely manner.

Recommendation 11
We recommend that OPM issue its "Information Security and Privacy Policy" to all agency employees and post a copy to the agency's internal website.

Comments
We concur. The document has been posted on THEO.

Recommendation 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

Comments
We concur with the thrust of the recommendation and will continue our efforts to reduce the use of SSNs and will update our formal plan to eliminate the unnecessary collection and use of SSNs.

Recommendation 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.

Comments
We concur.

Recommendation 14
We recommend that OPM continue its efforts to develop a methodology for logging computer-readable data extracts, and is unable to determine whether sensitive data has been erased after 90 days.

Comments
We concur with the need to continue the efforts to develop a methodology for logging computer-readable data extracts.

Recommendation 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.

Comments
We concur.

In addition, we have addressed the discovered vulnerabilities and provided the supporting documentation to the OIG.

Recommendation 16
We recommend that OPM continue its efforts in implementing all requirements of the FDCC.

Comments
We concur.

Recommendation 17
We recommend that OPM continue its efforts to ensure that all federal employees and contractors with access to OPM's IT resources complete IT security and privacy awareness training on an annual basis.

Comments
We concur. We are providing screenshots of our current status for the Security Awareness Training completion percentage from the GoLearn portal. Our current agency wide completion rate for Security Awareness Training is 98.32%.

Recommendation 18
We recommend that e-authentication risk assessments be completed for the required systems in accordance with OMB M-04-04.

Comments
We concur. We are providing thee-authentication risk assessment for eOPF to the OIG.

Recommendation 19
We recommend that the CIS/CIO promptly update OPM's IT security policies and publish them to THEO.

Comments
We concur that the CIS/CIO promptly update OPM's IT security policies and publish them to THEO. However, we disagree with the determination that this a material weakness.

OIG Comment:
"OPM did provide the OIG with an updated 'IT Security Policy Implementation Guide Incident Response and Reporting." However, this policy has not been updated on THEO. As a result, OPM employees do not have access to the most recent OPM policy on reporting data breaches."

Response: We disagree with this comment. "IT Security Policy Implementation Guide Incident Response and Reporting" that is posted on THEO is current. In addition, OPM

policy on reporting data breaches was provided to OPM employees and contractors by the agency Director in an email of November 5, 2007, entitled *New Procedures Regarding Personally Identifiable Information (PII)*. The email outlines policy and current processes for reporting actual or suspected data breaches. Furthermore, the same policy and instructions were posted to THEO at <u>http://theo.opm.gov/references/privacy/pii/reporting.asp</u> where OPM employees and contractors have access to them. In addition, all OPM employees completed mandatory training in May 2008 entitled *Personally Identifiable Information (PII) Responsibilities* that included the same policy and instructions for reporting data breaches. Finally, OPM employees and contractors have just completed the agency's online Security Awareness and Privacy Training for 2008 which contains the instructions for reporting data breaches. As noted in our comments on Recommendation 17, above, the training has been completed by more than 98.32% of agency employees and contractors.

<u>OIG Comment:</u>
"OPM has also developed a new "Information Security and Privacy Policy," that has been approved by OPM's senior management. Although this document provides updated information on several of the topics covered by the policies listed above, this document has not been published to THEO, and therefore cannot be readily accessed by OPM employees."

<u>Response:</u> The *IT Security Policy* has been replaced on THEO with the new policy titled *Information Security and Privacy Policy*.

<u>OIG Comment:</u>
"We acknowledge the steps that OPM has taken in creating updated policies and procedures, but will continue to consider this condition a material weakness in OPM's IT security program until all policies and procedures have been updated and published to THEO."

<u>Response:</u> The agency's *Information Security and Privacy Policy* have been published to THEO. In addition, the remainder of the documents cited were reviewed during February 2008 as part of an ongoing review of OPM's information security and privacy policy. We determined that the policies and procedures substantively represent current policies and practices and no immediate changes were deemed to be required. Furthermore, we are scheduling another review of these policies and procedures to ensure alignment in FY09.

Based on the information provided above we do not believe this weakness could be considered material.