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

Final Audit Report

Subject:

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT FY 2007

Report No: 4A-CI-00-07-007

Date: 09/18/2007

AUDIT REPORT

U.S. OFFICE OF PERSONNEL MANAGEMENT

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT
FY 2007

WASHINGTON, D.C.

Report No: 4A-CI-00-07-007

Date: 09/18/2007

Michael R. Esser
Assistant Inspector General
for Audits

EXECUTIVE SUMMARY

U.S. OFFICE OF PERSONNEL MANAGEMENT

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT
FY 2007

WASHINGTON, D.C.

Report No. 4A-CI-00-07-007

Date: 09/18/2007

This final audit report documents the Office of Personnel Management's (OPM's) continued efforts to manage and secure its information resources. Our conclusions and recommendations are detailed in the "Results" section of this report.

The results of this audit are summarized below:

- OPM appropriately maintains an inventory of all applications/systems under its control.
- The security controls for all systems were tested during fiscal year (FY) 2007.
- The contingency plans for 38 of OPM's 41 systems were tested during FY 2007.
- OPM performs routine oversight and evaluation of its major applications operated by a contractor.
- OPM has implemented an agency-wide plan of action and milestones process to help track and prioritize known information technology (IT) security weaknesses associated with the Agency's information systems.
- OPM has implemented a comprehensive certification and accreditation (C&A) process to ensure that the C&A of each Agency system remains active. An active C&A exists for all 41 systems at OPM.

- OPM has established a process for conducting privacy impact assessments (PIAs). As of September 2007, PIAs have been completed for each of the required 25 systems. However, 20 of the 25 have not been published to OPM's website.
- OPM has made significant progress in implementing the requirements of the Office of Management and Budget's Memorandum 06-15, "Safeguarding Personally Identifiable Information." However, OPM has not yet created an Agency-wide privacy policy, and has not completed its efforts in implementing technical controls to protect sensitive information.
- A technical configuration guide has been implemented to provide guidance for securing a variety of operating platforms in use at OPM.
- 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. However, several instances of policy violation indicate that OPM should pursue additional education and training for its employees and contractors related to incident response.
- OPM has implemented a process to provide annual and mandatory information technology security and privacy awareness training.
- The security and privacy awareness 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.
- OPM's IT security policies have not been updated since November 2004. The Office of the Inspector General considers this condition to be a material weakness in the internal control structure of OPM's IT security program.

CONTENTS

Page

Introduction

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

Background

FISMA requirements pertain to all information systems (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-07-19 (FY 2007 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 Plan Testing
- Agency Oversight of Contractor Systems
- Agency Plan of Action and Milestones Process
- Certification and Accreditation Process
- Agency Privacy Program and Privacy Impact Assessment Process
- Configuration Management
- Incident Reporting
- Security Awareness Training
- Peer-to-Peer File Sharing

- E-authentication Risk Assessments

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

This performance audit was conducted by the Office of the Inspector General (OIG) in accordance with government auditing standards issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures that we considered necessary. The audit covered OPM's FISMA compliance efforts through September 2007.

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:

- Government Financial Information System (OIG Report No. 4A-CF-00-07-010)
- GoLearn Learning Management Systems (OIG Report No. 4A-HR-00-07-09)
- Actuaries Group System (OIG Report No. 4A-RI-00-07-41)
- Learning Management System (OIG Report No. 4A-HR-07-42)

In addition, the FY 2007 FISMA Follow-up Audit (OIG Report No. 4A-CI-00-07-008) indicated that the following OPM major applications had outstanding audit recommendations from the FY 2006, FY 2005, and FY 2004 FISMA audits:

- Fingerprint Transaction System
- OPM Personnel Investigation Processing System Imaging System
- Electronic Individual Retirement Record
- Human Resources Historical Data Warehouse
- Enterprise Human Resources Integration Data Warehouse
- USA Jobs
- Electronic Questionnaire for Investigations Processing
- PIPS Financial Interface System
- Benefits Financial Management 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.

We also relied on the work performed by KPMG during its audit of OPM's financial statements. KPMG's audit of the general controls environment of OPM's computer systems was designed from procedures contained in the U.S. Government Accountability Office's Federal Information System Controls Audit Manual (FISCAM).

Details of our audit can be found in the "Results" section of this report. We discussed these results at an exit conference with OPM officials and in a draft report. 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 Memorandum M-07-19, "FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management";
- 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, "Recommended Security Controls for Federal Information Systems";
- NIST SP 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories";
- OMB Memorandum M-06-16, "Protection of Sensitive Agency Information";
- OMB Memorandum M-06-15, "Safeguarding Personally Identifiable Information";
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies";
- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources";
- Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"; and
- Other criteria as appropriate.

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

sufficient to achieve the audit objectives. Except as noted above, the audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States.

As appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

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 2007 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

This section details the results of our audit of OPM's FISMA compliance efforts. The results are formatted to be consistent with the questions asked in the FY 2007 OMB FISMA OIG reporting instructions.

I. System Inventory

OPM identified 41 major applications/systems within 8 of its program offices. The Center for Information Services and Chief Information Officer (CIS/CIO) continuously maintains an inventory of OPM's systems, and the OIG agrees with the total listed in the most recent system inventory. The CIS/CIO relied on the various program offices to identify and report systems to be included in the agency's universe of systems. The OIG reviewed OPM's system inventory and determined that 30 of these operated within the agency and 11 are operated at a contractor facility. We also reviewed the list of systems identified in OPM's IT architecture document and found that each of these systems is identified or covered by the applications listed in OPM's system inventory.

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

1. Certification and Accreditation

A certification and accreditation (C&A) has been completed and remains active for each of the 41 systems in OPM's inventory. See section **V** below for details of OPM's C&A process.

2. Security Controls Testing

The CIS/CIO at OPM has implemented procedures for conducting an annual review of system security controls. 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 received a test of security controls for all 41 OPM systems in FY 2007. We judgmentally selected 5 of these 41 systems and conducted a detailed review of their FY 2007 security controls tests. We found that the sample security controls tests were completed in accordance with NIST SP 800-53 guidance. The results of this sample were not projected to the entire population.

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 . . . ."

Self-assessments and security control tests provide 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 self-assessment and a security controls test increases the risk that agency officials may be unable to make informed judgments that appropriately mitigate risks to an acceptable level.

3. Contingency Planning

The CIS/CIO emphasizes the importance of developing and testing contingency plans for OPM's systems. FISMA requires that the contingency plan of each major application be tested on an annual basis. However, the OIG did not receive contingency plan tests for 3 of OPM's 41 systems in FY 2007.

The OIG judgmentally selected a sample of 5 of the 38 contingency plans received 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". 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.

Effective contingency planning and testing establishes procedures and technical measures that enable a system to be recovered quickly and effectively following a service disruption or disaster. Thus, an incomplete or untested contingency plan increases the risks of system and service unavailability.

Recommendation 1

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

CIS/CIO Response:

"The three remaining systems, GoLearn GeoLearning Baseline LMS GSS, GoLearn Learn Baseline LMS GSS, and GoLearn Intekras/GP/SABA Baseline LMS GSS, will have contingency plans testing completed by September 14, 2007 and submission of documentation shortly thereafter. We request that the OIG review these documents as they come in and update the completion tables in the report to accurately reflect status through September 14, 2007."

OIG Reply:

Due to the constraints of the FISMA reporting timeline, the OIG is unable to review documentation provided after the September 7th deadline agreed upon by the CIS/CIO and OIG. We continue to recommend that OPM's program offices test the contingency plans for each system on an annual basis.

III. Agency Oversight of Contractor Systems

The OIG agrees with OPM's assessment of the number of systems operated by a contractor.

OPM performs routine oversight and evaluation of its major applications operated by a contractor. Each of the 11 OPM systems that are operated by a contractor have been certified and accredited by the Agency. In addition, the annual self-assessment review of IT security controls for each of these systems was conducted or reviewed by an OPM employee.

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. OPM has implemented an agency-wide POA&M process to help track known IT security weaknesses associated with the Agency's information systems. The CIS/CIO has created a spreadsheet template to assist in the development of POA&Ms.

OPM program office officials develop, implement, and manage POA&Ms for each system that they own and operate. On a quarterly basis, program officials send the CIS/CIO an updated POA&M detailing the progress made in correcting the system's security weaknesses. The CIS/CIO centrally tracks all OIG audit recommendations to ensure that they are incorporated into the POA&M process.

In addition, each program office 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.

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 must renew its C&A every three years.

OPM has implemented a comprehensive C&A process to ensure that the C&A of each Agency system remains active. Furthermore, OPM's Information Technology Security Officer has implemented a process to review C&A packages and provide feedback to program offices. The OIG found that all OPM agency systems have complete and up-to-date certification and accreditation packages.

The OIG conducted a detailed review of the 16 C&A packages that were completed during FY 2007. Nothing came to our attention to indicate that OPM's C&A process is not in compliance with relevant FISMA requirements and NIST guidance.

VI. Agency Privacy Program and Privacy Impact Assessment Process

The FY 2007 FISMA reporting instructions require the OIG to evaluate OPM's privacy impact assessment process and its privacy program in terms of its progress in implementing the provisions of OMB Memorandum M-06-15.

1. Privacy Impact Assessments

The E-Government Act of 2002, section 208, requires agencies to conduct privacy impact assessments (PIA) of information systems that process personally identifiable information (PII). OPM's IT security officer issued a "PII Questionnaire" to the designated security officers for each of the Agency's major systems to determine whether the system contains PII. The results of the questionnaire indicated that 35 systems required PIAs. Since the time this questionnaire was issued, adjustments to the inventory have been made and there are currently 37 systems that contain PII. Of these 37 systems, 25 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 September 2007, 5 of the 25 (20%) required PIAs had been published to OPM's website. Of the 20 outstanding PIAs, all have been reviewed and signed by the CIO and are in queue to be approved for publication.

Recommendation 2

We recommend that OPM's PPG continue its efforts to publish PIAs for all required systems.

CIS/CIO Response:

"Concur, however, recommend changing the above paragraph to accurately reflect the number of systems requiring PIAs."

OIG Reply:

We have incorporated the updated information provided by OPM's PPG on September 6, 2007 into this report, and continue to recommend PPG continue its efforts to publish PIAs for all required systems.

2. Privacy Program - Implementation of OMB M-06-15

OMB Memorandum M-06-15, "Safeguarding Personally Identifiable Information," requires agencies to review the administrative, technical, and physical safeguards that protect PII. The OIG documented the efforts OPM has made in each of these areas.

Administrative Controls

OMB M-06-15 requires that each agency's Senior Official for Privacy conduct a review of its policies and processes, and take corrective action as appropriate. OPM does not currently have an Agency-wide "privacy policy" in place to fully address the protection of PII on Agency systems. OPM's PPG is currently working to create such a policy.

Recommendation 3

We recommend that OPM's PPG continue its efforts to develop an Agency-wide privacy policy.

CIS/CIO Response:

"Concur."

Technical Controls

In an effort to meet the requirements of OMB Memorandum M-06-16, "Protection of Sensitive Agency Information," OPM has implemented several technical controls to ensure the protection of sensitive data:

- Backup tapes sent to an offsite location are encrypted
- OPM employees are instructed to manually encrypt sensitive data on mobile workstations by utilizing [redacted] encryption technology
- Data at rest on [redacted] handheld devices is encrypted

Furthermore, OPM is in the process of testing and implementing several additional technical controls:

- Automatically encrypting PII on mobile workstations
- Requiring two-factor authentication to access PII on OPM's systems

Recommendation 4

We recommend that OPM continue its efforts to protect sensitive data by implementing technical controls in compliance with OMB Memorandum M-06-16.

CIS/CIO Response:

"Concur."

Physical Controls

OPM has implemented a variety of physical controls at its facilities to ensure the protection of PII in physical form (i.e. printed). In addition, OPM has installed "shred bins" throughout the facilities. Employees are instructed to place documents containing PII into these locked bins, which will securely store the documents until they are appropriately destroyed.

VII. Configuration Management

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]

[redacted] operating platforms. Furthermore, OPM's Application Systems Group (ASG) has implemented configuration guides for securing its [redacted] databases.

The configuration of OPM's [redacted] platforms have been reviewed by the OIG as part of the FY 2005 FISMA audit. Since there have been no major changes in these systems, they were not re-reviewed in FY 2007. However, the OIG did conduct a review of the configuration of several [redacted] databases.

[redacted] Databases

OPM has developed an [redacted] Configuration Policy to provide guidance in securing the [redacted] databases that are part of the Agency's major application. The OIG conducted a vulnerability scan of four [redacted] databases at OPM, and found several instances where the requirements of the [redacted] Configuration Policy were not implemented.

As of August 2007, three of these databases have been updated to include the latest [redacted] patch set, but had not been updated with the latest critical patch update (CPU) as required by OPM's [redacted] Configuration Policy.

Recommendation 5

We recommend that OPM install the latest [redacted] CPUs for all [redacted] databases.

CIS/CIO Response:

"We have completed installing the latest [redacted] CPUs for all [redacted] databases. Documentation showing evidence that these patches were completed was provided to OIG on August 30, 2007. We ask that you delete this recommendation."

OIG Reply:

We have reviewed the documentation provided in response to our draft audit report, and agree that the appropriate patches have been installed on the four databases reviewed during this audit. We will follow up on this recommendation by testing additional databases in the FY 2008 FISMA audit.

VIII. Incident Reporting

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

Internal Reporting

OPM's Incident Response and Reporting Policy requires the users of the Agency's IT resources to immediately notify OPM's help desk when IT security incidents occur.

Although this requirement is reiterated in OPM's annual IT security and privacy awareness training, the OIG believes that additional emphasis should be placed on the education of employees and contractors regarding the appropriate handling of security incidents.

During its 2007 financial statement audit, KPMG reported that three incidents involving PII were not reported to the OPM help desk in a timely manner. The incidents were reported from eight to forty-nine days after being initially identified. In addition, the OIG is aware of one major IT security incident related to the USA Jobs system that was not reported to the help desk in a timely manner.

OPM's Incident Response and Reporting Policy also outlines the various Agency officials that should be notified after security incidents are reported to the help desk. This list includes the Assistant Inspector General for Investigations in the OIG. However, the OIG was not properly notified of security incidents at OPM throughout FY 2007. OPM officials are aware of this issue and are working to create new procedures for notifying the appropriate individuals when security incidents occur. In August 2007, an OIG representative was added to OPM's incident notification email distribution list.

Recommendation 6

We recommend that the CIS/CIO provide additional education to OPM employees and contractors emphasizing the need to immediately notify the help desk when IT security incidents are detected. This education could come in the form of routine reminders through email or the Director's monthly OPMomentum newsletters.

CIS/CIO Response:

"Concur. CIS will continue to review different avenues to remind OPM employees and contractors of the responsibility of notifying the OPM Help Desk of the loss of sensitive information, including PII, in accordance with US-CERT guidelines."

Recommendation 7

We recommend that OPM's help desk and CIRT continue its efforts in notifying the appropriate individuals and offices within the Agency when security incidents occur. We recommend that the CIRT provide the OIG with a monthly summary of security incidents, and develop a procedure to judgmentally provide immediate notification to the OIG of serious security incidents.

CIS/CIO Response:

"Concur, however, the delay was in the reporting of incidents by OPM employees and contractors and represents policy violations, not necessarily an intrinsic deficiency in the Incident Response program. Once reported to the agency, it was reported within the required timeline established by US-CERT. CIS will work to refine its incident response procedures to ensure serious security incidents are reported immediately to OIG and appropriate program offices."

US-CERT Reporting

The Incident Response and Reporting policy states that OPM's CIRT is responsible for preparing 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.

Law Enforcement Reporting

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.

IX. Security Awareness Training

The CIS/CIO at OPM has implemented a process to provide annual and mandatory information technology security and privacy awareness training. The training must be completed by all federal employees and contractors with access to OPM's IT resources.

The training is conducted through an interactive online course provided through OPM's eLearning website (http://elearning.opm.gov). The course introduces employees and contractors to the basic concepts of computer security. 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 2007, 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 20, 2007. As of August 2007, 5,774 out of 5,938 (97%) employees and contractors have completed the training.

Individuals with significant IT security responsibilities are required to receive additional training. The CIS/CIO maintains records of this additional training to ensure that all training requirements are met.

X. Peer-to-Peer File Sharing

FISMA requires agencies to implement policies regarding the use of peer-to-peer file sharing on its networks. All OPM employees and contractors are required to take an online IT security and privacy awareness training course (see section IX, above). This training course

contains a section that defines peer-to-peer file sharing, and explicitly prohibits its use on OPM networks and workstations.

XI. E-authentication Risk Assessments

OPM has not fully completed system e-authentication risk assessments in accordance with OMB guidance.

OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," states that it "applies to remote authentication of human users of Federal agency IT systems for the purposes of conducting government business electronically (or e-government)," and requires agencies to conduct an e-authentication risk assessment of the e-government system. OPM officials and the OIG agree that four of the Agency's systems are subject to e-authentication requirements.

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.

The e-authentication risk assessment for two of the OPM systems utilized Carnegie Mellon University's "e-Authentication Risk and Requirements Assessment Database" tool. The e-authentication risk assessment for the third system was conducted by a contractor using a proprietary template. The OIG verified that each of these e-authentication risk assessments satisfy the requirements of M-04-04.

However, the OIG was not provided with an e-authentication risk assessment for the fourth system, and the traditional risk assessment for this system was not completed in accordance with OMB M-04-04. Specifically, the risk assessment for this system did not identify the various transactions of the system to map each of them to one of four assurance levels outlined in M-04-04.

Recommendation 8

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

CIS/CIO Response:

"The fourth e-Authentication Risk Assessment was provided to OIG on September 4, 2007. We ask that you delete this recommendation."

OIG Reply:

We reviewed the additional e-Authentication Risk Assessment provided in response to our draft audit report, and agree that OPM is now compliant with the requirements of FISMA and OMB M-04-14. This recommendation does not require further action at this time, but will remain in this audit report to document the timeline of OPM's compliance efforts.

XII. Security and 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.

OPM's IT security policies have not been updated since November 2004. This issue was highlighted in the OIG's FY 2005 and FY 2006 FISMA reports, where the OIG recommended that the CIS/CIO develop a formal process to analyze new guidance and update OPM's IT security policies accordingly. Although the CIS/CIO states that they are currently in the process of updating these policies, they continue to remain outdated. The OIG considers this condition to be a material weakness in the internal control structure of OPM's IT security program.

OPM's IT security policies and procedures are the basis for the agency's security program and provide agency officials guidance in implementing the program. Furthermore, OMB FY 2007 FISMA Reporting Instructions require agencies to follow NIST standards and guidance. By having a formal process to promptly and accurately update OPM's IT security policies and procedures based on changes or additions recommended by new guidance, OPM personnel will understand their roles and responsibilities and can consistently implement the new guidance. Consequently, OPM's IT security program will accurately reflect the initiatives set forth by the new guidance, thereby strengthening OPM's IT security.

Recommendation 9

We recommend that the CIS/CIO promptly update OPM's IT security policies.

CIS/CIO Response:

"Concur."

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

APPENDIX A

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Management Services
Division

SEP 7 2007

MEMORANDUM FOR [redacted]
Chief, Information Systems Audits Group

FROM: JANET L. BARNES
Chief Information Officer

Subject: FY 2007 Federal Information Security Management Act Audit

Thank you for giving us the opportunity to review your draft FY 2007 Federal Information Security Management Act (FISMA) Audit Report, Report No: 4A-CI-00-07-007, dated August 21, 2007. In our detailed review (attached), we have provided comments on a number of the items. Once your report is finalized, we will ensure that every recommendation that should appropriately be addressed in a POA&M is reflected in the next quarterly POA&M updates.

FY 2007 was a very dynamic year for the program offices in regards to the numerous additional security requirements set by the Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST). Additional security measures were required to be implemented by the program offices to ensure the protection of personally identifiable information (PII) in OPM information systems. They were also required to be in compliance with the new NIST Special Publication 800-53 security controls by February 2007, in addition to a more in-depth annual self-assessment imposed by NIST and the IT Security Officer. Additionally, of the 41 major systems at OPM, 16 were re-accredited in FY 2007 for continued operation, including the two major infrastructures.

We have made significant improvements to our IT Security Program in FY 2007 and continue to believe that we are adequately protecting OPM information systems. We recognize that additional steps can be taken to protect our critical IT assets against the ever expanding list of security threats and appreciate recommendations to improve or enhance our IT Security Program even further.

If you have any questions on these comments or would like to arrange a meeting to discuss them, please contact OPM's IT Security Officer, [redacted], at [redacted].

Attachment

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

******Text from OIG draft audit report deleted by OIG******

Recommendation 1

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

FY 2007 CIS Response:

The three remaining systems, [redacted], will have contingency plans testing completed by September 14, 2007 and submission of documentation shortly thereafter. We request that the OIG review these documents as they come in and update the completion tables in the report to accurately reflect status through September 14, 2007.

VI. Agency Privacy Program and Privacy Impact Assessment Process

******Text from OIG draft audit report deleted by OIG******

Recommendation 2

We recommend that OPM's PPG continue its efforts to publish PIAs for all required systems.

FY 2007 CIS Response:

Concur, however, recommend changing the above paragraph to accurately reflect the number of systems requiring PIAs. It should read as follows, per the September 6, 2007 memorandum from Chief, Plans and Policies Groups:

"The E-Government Act of 2002, section 208, requires agencies to conduct privacy impact assessments (PIA) of information systems that process personally identifiable information (PII). OPM's IT security officer issued a "PII Questionnaire" to the designated security officers for each of the Agency's major systems to determine whether the system contains PII. The results of the questionnaire indicated that 35 systems contained PII. Since the time this questionnaire was issued, adjustments to the inventory have been made and currently there are 37 systems that contain PII. Of these 37 systems, 25 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 September 2007, 5 of the 25 (20%) required PIAs have been published to OPM's website. Of

the 20 outstanding PIAs, all have been reviewed and signed by the CIO and are in the queue to be approved for publication."

******Text from OIG draft audit report deleted by OIG******

Recommendation 3

We recommend that OPM's PPG continue its efforts to develop an Agency-wide privacy policy.

FY 2007 CIS Response: Concur.

******Text from OIG draft audit report deleted by OIG******

Recommendation 4

We recommend that OPM continue its efforts to protect sensitive data by implementing technical controls in compliance with OMB Memorandum M-06-16.

FY 2007 CIS Response: Concur.

VII. Configuration Management

******Text from OIG draft audit report deleted by OIG******

Recommendation 5

We recommend that OPM install the latest [redacted] CPUs for all [redacted] databases.

FY 2007 CIS Response: We have completed installing the latest [redacted] CPUs for all [redacted] databases. Documentation showing evidence that these patches were completed was provided to OIG on August 30, 2007. We ask that you delete this recommendation.

VIII. Incident Reporting

******Text from OIG draft audit report deleted by OIG******

Recommendation 6

We recommend that the CIS/CIO provide additional education to OPM employees and contractors emphasizing the need to immediately notify the help desk when IT security incidents are detected. This education could come in the form of routine reminders through email or the Director's monthly OPM momentum newsletters.

FY 2007 CIS Response: Concur. CIS will continue to review different avenues to remind OPM employees and contractors of the responsibility of notifying the OPM Help Desk of the loss of sensitive information, including PII, in accordance with US-CERT guidelines.

Recommendation 7

We recommend that OPM's help desk and CIRT continue its efforts in notifying the appropriate individuals and offices within the Agency when security incidents occur. We recommend that the CIRT provide the OIG with a monthly summary of security incidents, and develop a procedure to judgmentally provide immediate notification to the OIG of serious security incidents.

FY 2007 CIS Response: ***Concur, however, the delay was in the reporting of incidents by OPM employees and contractors and represents policy violations, not necessarily an intrinsic deficiency in the Incident Response program. Once reported to the agency, it was reported within the required timeline established by US-CERT. CIS will work to refine its incident response procedures to ensure serious security incidents are reported immediately to OIG and appropriate program offices.***

XI. E-authentication Risk Assessments

******Text from OIG draft audit report deleted by OIG******

Recommendation 8

We recommend that e-authentication risk assessments be completed for the required systems at OPM in accordance with OMB M-04-14.

FY 2007 CIS Response: ***The fourth e-Authentication Risk Assessment was provided to OIG on September 4, 2007. We ask that you delete this recommendation.***

XII. Security and Policies and Procedures Review and Update

******Text from OIG draft audit report deleted by OIG******

Recommendation 9

We recommend that the CIS/CIO promptly update OPM's IT security policies.

FY 2007 CIS Response: ***Concur.***

APPENDIX B

OMB FISMA REPORTING TEMPLATE FOR INSPECTORS GENERAL

Section C - Inspector General: Questions 1 and 2

Agency Name: U.S. Office of Personnel Management **Submission date:** 18-Sep-07

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
Human Resources Line of Business	High	0	0	2	2	2	2	2	100%	2	100%	2	100%
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**2**	**2**	**2**	**2**	**2**	100%	**2**	100%	**2**	100%
Office of the Chief Financial Officer	High					0	0						
	Moderate	3	3			3	3	3	100%	3	100%	3	100%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**3**	**3**	**0**	**0**	**3**	**3**	**3**	100%	**3**	100%	**3**	100%
Division for Strategic Human Resources Policy	High					0	0						
	Moderate	2	2			2	2	2	100%	2	100%	2	100%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**2**	**2**	**0**	**0**	**2**	**2**	**2**	100%	**2**	100%	**2**	100%
Division for Human Resources Products and Services	High					0	0						
	Moderate	13	13	7	7	20	20	20	100%	20	100%	17	85%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**13**	**13**	**7**	**7**	**20**	**20**	**20**	100%	**20**	100%	**17**	85%
Federal Investigative Services Division	High	4	4			4	4	4	100%	4	100%	4	100%
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**4**	**4**	**0**	**0**	**4**	**4**	**4**	100%	**4**	100%	**4**	100%
Division for Human Capital Leadership & Merit System Accountability	High					0	0						
	Moderate	1	1			1	1	1	100%	1	100%	1	100%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**1**	**1**	**0**	**0**	**1**	**1**	**1**	100%	**1**	100%	**1**	100%
Division for Management Services	High	1	1			1	1	1	100%	1	100%	1	100%
	Moderate	3	3	2	2	5	5	5	100%	5	100%	5	100%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**4**	**4**	**2**	**2**	**6**	**6**	**6**	100%	**6**	100%	**6**	100%
Office of the Inspector General	High					0	0						
	Moderate	3	3			3	3	3	100%	3	100%	3	100%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**3**	**3**	**0**	**0**	**3**	**3**	**3**	100%	**3**	100%	**3**	100%
Agency Totals	**High**	**5**	**5**	**2**	**2**	**7**	**7**	**7**	100%	**7**	100%	**7**	100%
	Moderate	**25**	**25**	**9**	**9**	**34**	**34**	**34**	100%	**34**	100%	**31**	91%
	Low	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
	Total	**30**	**30**	**11**	**11**	**41**	**41**	**41**	100%	**41**	100%	**38**	93%

Section C - Inspector General: Question 3

Agency Name: U.S. 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)	Agency or Contractor system?

Number of known systems missing from inventory:	

Section C - Inspector General: Questions 4 and 5

Agency Name: U.S. 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.	Almost Always (96-100% 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).	Almost Always (96-100% of the time)
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always (96-100% of the time)
4.e.	IG findings are incorporated into the POA&M process.	Almost Always (96-100% 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: See FY 2007 Federal Information Security Management Act Audit - Section IV

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 Information 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	Excellent	
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: See FY 2007 Federal Information Security Management Act Audit - Section V

Section C - Inspector General: Questions 6 and 7

Agency Name:	**U.S. Office of Personnel Management**	
	Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process	
6.a.	**Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D II.4 (SAOP reporting template), including adherence to existing policy, guidance, and standards.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing **Comments: See FY 2007 Federal Information Security Management Act Audit - Section VI**	Satisfactory
6.b.	**Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15, "Safeguarding Personally Identifiable Information" since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect personally identifiable information (PII).** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing **Comments: See FY 2007 Federal Information Security Management Act Audit - Section VI**	**Good**
	Question 7: Configuration Management	
7.a.	**Is there an agency-wide security configuration policy? Yes or No.** **Comments**:	Yes
7.b.	**Approximate the extent to which applicable information systems apply common security configurations established by NIST.** **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)
	Section C - Inspector General: Questions 8, 9, 10 and 11	
Agency Name:	**U.S. Office of Personnel Management**	
	Question 8: 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.		
8.a.	**The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.**	No
8.b.	**The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)**	Yes
8.c.	**The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.**	Yes

Comments: The OIG was not properly notified of security incidents at OPM throughout FY 2007. In August 2007, an OIG representative was added to OPM's incident notification email distribution list. **See FY 2007 Federal Information Security Management Act Audit - Section VII**	
Question 9: 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 10: Peer-to-Peer File Sharing	
Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	**Yes**
Question 11: E-Authentication Risk Assessments	
The agency has completed system e-authentication risk assessments. Yes or No.	**Yes**