U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Subject:

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S ELECTRONIC OFFICIAL PERSONNEL FOLDER FY 2009

Report No. 4A-HR-00-09-032

Date: June 2, 2009

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S ELECTRONIC OFFICIAL PERSONNEL FOLDER FY 2009

WASHINGTON, D.C.

Report No. 4A-HR-00-09-032

Date: June 2, 2009

Michael R. Esser
Assistant Inspector General
for Audits

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S ELECTRONIC OFFICIAL PERSONNEL FOLDER FY 2009

WASHINGTON, D.C.

Report No. 4A-HR-00-09-032

Date: June 2, 2009

This final audit report discusses the results of our review of the information technology security controls of the Electronic Official Personnel Folder (eOPF) System. The OIG found nothing to indicate that eOPF is not in full compliance with all applicable requirements. Our conclusions are detailed in the "Results" section of this report.

The results of our audit are summarized below:

- A self-assessment was not required for eOPF in fiscal year (FY) 2008. The Office of the Inspector General (OIG) will verify that a current self-assessment of National Institute of Standards and Technology (NIST) Special Publication 800-53 controls is conducted for this system as part of the FY 2009 general Federal Information Security Management Act audit process.
- A risk assessment was performed for eOPF that encompasses the nine primary steps outlined in NIST guidance.
- The eOPF information system security plan was prepared in accordance with the format and methodology outlined in NIST guidance.
- An independent system security test and evaluation was conducted for eOPF.

- eOPF was certified and accredited in FY 2009 in accordance with NIST guidance.
- The eOPF contingency plan is routinely maintained and tested in accordance with NIST Guidance.
- An impact analysis based on the Federal Information Processing Standards Publication 199 was completed for eOPF in accordance with NIST guidance. The OIG agreed with the "high" classification of the system.
- The OIG did not detect any weaknesses in eOPF's security controls that were not already identified in the Plan of Action and Milestones (POA&M) for the system.
- The 2009 first quarter POA&M for eOPF appeared to be properly maintained in accordance with Office of Personnel Management policy and guidance from the U.S. Office of Management and Budget.

Contents

Introduction

On December 17, 2002, the President signed into law the E-Government Act (P.L. 107-347) which includes Title III, the Federal Information Security Management Act (FISMA). It 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 evaluated the information technology (IT) security controls related to the Office of Personnel Management's (OPM) Electronic Official Personnel Folder (eOPF).

Background

eOPF is one of OPM's 41 critical IT systems. As such, FISMA requires that the Office of the Inspector General (OIG) perform an audit of IT security controls of this system, as well as all of the agency's systems on a rotating basis.

The Human Resources Line of Business (HRLOB) has been designated with ownership of eOPF. eOPF is a web-based application that allows Federal employees and agency human resources professionals to view digital copies of documents related to employment actions and history of individuals employed by the Federal government. HRLOB grants its customer agencies access to the system and the ability to create accounts for its employees to access their own personnel records.

Although the eOPF application is owned and administered by OPM's HRLOB, the infrastructure supporting eOPF is owned and maintained by the Department of the Interior's (DOI) National Business Center (NBC). The technical infrastructure in place at the NBC has been certified and accredited by DOI.

This was our first audit of the security controls surrounding eOPF. We discussed the results of our audit with HRLOB representatives at an exit conference.

Objectives

Our overall objective was to perform an evaluation of security controls for eOPF to ensure that HRLOB officials have implemented IT security policies and procedures in accordance with standards established by OPM's Center for Information Services (CIS).

These policies and procedures are designed to assist program office officials in developing and documenting IT security practices that are in substantial compliance with FISMA, as well as OMB regulations and the National Institute of Standards and Technology (NIST) guidance.

OPM's IT security policies and procedures require managers of all major and sensitive systems to complete a series of steps to (1) certify that their system's information is adequately protected and (2) authorize the system for operations. The overall audit objective was accomplished by

reviewing the degree to which a variety of these security program steps have been implemented for eOPF, including:

- Annual Self Assessments;
- Risk and Vulnerability Assessments;
- Information System Security Plans;
- Independent Security Test and Evaluation;
- Certification and Accreditation;
- Contingency Planning;
- Federal Information Processing Standards Publication 199 (FIPS 199) Analysis;
- Evaluation of NIST Special Publication (SP) 800-53 Security Controls; and
- Plan of Action and Milestones Process.

Scope and Methodology

Our performance audit was conducted 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 FISMA compliance efforts of HRLOB officials responsible for eOPF, including IT security controls in place as of February 2009.

We considered the eOPF internal control structure 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.

To accomplish our objective, we interviewed representatives of OPM's HRLOB office and other program officials with eOPF security responsibilities. We reviewed relevant OPM IT policies and procedures, Federal laws, OMB policies and guidance, and NIST guidance. As appropriate, we conducted compliance tests to determine the extent to which established controls and procedures are functioning as required.

Details of the security controls protecting the confidentiality, integrity, and availability of eOPF are located in the "Results" section of this report. Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the eOPF system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM IT Security Policy,
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources,
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- NIST SP 800-12, An Introduction to Computer Security,
- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems;

- NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems;
- NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems;
- NIST SP 800-60 Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories;
- Federal Information Processing Standard (FIPS) 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 information 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.

The audit was performed by the OPM Office of the Inspector General, as established by the Inspector General Act of 1978, as amended. The audit was conducted from January through March 2009, in OPM's Washington, D.C. office.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether HRLOB's management of eOPF is consistent with applicable standards. Nothing came to the OIG's attention during this review to indicate that HRLOB is in violation of relevant laws and regulations.

Results

This section details the results of our audit of eOPF.

I. Self-Assessment

FISMA requires that the IT security controls of each major application owned by a Federal agency be tested on an annual basis. Security control self-assessments provide a method for agency officials to evaluate the current status of the security controls of their systems and, when necessary, establish a target for improvement. However, in July 2008, an independent contractor tested eOPF's management, operational, and technical controls, as outlined in NIST SP 800-53 (see section IV, below). Therefore, an internal self-assessment of these controls was not required in fiscal year (FY) 2008.

The OIG will verify that a current self-assessment of NIST SP 800-53 controls is conducted for this system as part of the FY 2009 general FISMA audit process.

II. Risk Assessment

A risk management methodology focused on protecting core business operations and processes is a key component of an efficient IT security program. A risk assessment is used as a tool to identify security threats, vulnerabilities, potential impacts, and probability of occurrence. In addition, a risk assessment is used to evaluate the effectiveness of security policies and recommend countermeasures to ensure adequate protection of information technology resources.

NIST offers a nine step systematic approach to conducting a risk assessment that includes: (1) system characterization; (2) threat identification; (3) vulnerability identification; (4) control analysis; (5) likelihood determination; (6) impact analysis; (7) risk determination; (8) control recommendation; and (9) results documentation.

HRLOB contracted an outside vendor to conduct a risk assessment for eOPF that was based on NIST SP 800-30, Risk Management Guide for Information Technology Systems. The eOPF risk assessment was performed in December 2008 and encompassed the nine elements outlined above.

In addition, a privacy impact assessment (PIA) was conducted for eOPF in November 2008. A PIA is used to ensure that no collection, storage, access, use, or dissemination of personally identifiable information occurs that is not needed or authorized.

III. Information System Security Plan

The completion of an information system security plan (ISSP) is a requirement of OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources. In order to assist agencies in establishing a standardized approach to developing an ISSP,

NIST developed SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems.

The ISSP for eOPF was prepared in December 2008 in accordance with the format and methodology outlined in NIST SP 800-18, and contained all major elements suggested by the guidance.

IV. Independent Security Test and Evaluation

The purpose of an independent security test and evaluation (ST&E) is to determine whether the IT system is compliant with the security requirements documented in its security plan, and to verify that the security controls identified in the plan are correctly implemented and effective.

An ST&E was completed for eOPF during June and July 2008 as part the system's FY 2009 certification and accreditation (C&A) process. The ST&E was conducted by Carson Associates, a company independent of both OPM and the DOI NBC that hosts eOPF. The OIG verified that the test included a review of the appropriate management, operational, and technical controls required for a system with a "high" security categorization according to NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems.

Several NIST SP 800-53 controls were identified by Carson Associates as not applicable to the eOPF C&A. Carson Associates stated that these controls related to the hardware infrastructure maintained by the NBC, and therefore referred to the NBC C&A package for an assessment of these controls. The OIG evaluated the appropriateness of deferring these controls to the NBC, and did not disagree with Carson Associates' assessment.

In addition, several NIST SP 800-53 controls are related to agency-level policies and procedures. When evaluating these controls, Carson Associates deferred to the relevant OPM IT security policies or procedures posted to OPM's internal web site. However, several of the OPM policies referenced in the ST&E are extremely outdated, and the OIG believes that this represents a security weakness to any IT system that is subject to the requirements outlined in these documents. Specifically, the following outdated policies were referenced in the ST&E for eOPF:

- OPM Certification and Accreditation Process
- OPM IT Security Guide - Security Documentation Guide
- OPM Security Plan Implementation Guide
- Policy on Information Technology Procurement
- OPM System Access Authorization Procedures
- OPM IT Security Guide - Incident Response and Reporting

The maintenance of these policies and procedures is the responsibility of OPM's CIS. The OIG recommended in its FY 2008 FISMA audit report that these documents be updated, and therefore will not include this weakness as an audit finding in this report. However,

HRLOB should evaluate the impact that any outdated information contained in these policies has on the security controls of eOPF.

The remaining NIST SP 800-53 controls were within the scope of the ST&E, and Carson Associates determined whether each control was satisfied or not satisfied. Carson Associates presented a copy of the evaluation results to HRLOB and helped the program office incorporate the identified weaknesses into the eOPF risk assessment.

V. Certification and Accreditation

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, states that 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. eOPF was certified and accredited on January 7, 2009 in accordance with NIST SP 800-37 requirements.

OPM's Certifying Official and IT security officer evaluated the security-related documentation that HRLOB provided in the certification package. The Certifying Official stated that the requirements for certification have been satisfied, and suggested that the program office determine whether it is appropriate to formally accept certain risks identified during the C&A process.

The certification package was also reviewed by the Director of HRLOB, who was acting as the system's Authorizing Official. The Authorizing Official reviewed the security controls that have been implemented for the system, weighed the remaining residual risks against the operational requirements, and granted a three year Authorization to Operate to the eOPF major application.

VI. Contingency Planning

NIST SP 800-34, Contingency Planning Guide for IT Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. The OPM IT security policy requires that OPM general support systems and major applications have viable and logical disaster recovery and contingency plans, and that these plans are annually reviewed, tested, and updated

eOPF is hosted at the DOI NBC, and the IT infrastructure supporting this system is under the control and governance of the NBC. In the event of a disaster, the NBC will perform all tasks associated with restoring communications, network infrastructure, servers, and applications. The OPM/HRLOB Operations Team will provide oversight, guidance, and minor application-specific configurations during the restoration phase of the disaster recovery process, and will also provide application functionality testing of the restored systems.

The contingency plan developed for eOPF has been tested and reviewed by both the NBC and HRLOB Operations Team members. The plan addresses all of the key elements outlined in the NIST guide

VII. Federal Information Processing Standards Publication 199 Analysis

FIPS 199 establishes three potential levels of impact (low, moderate, and high) relevant to securing Federal information and information systems for each of three primary security objectives (confidentiality, integrity, and availability).

NIST SP 800-60 Volume II, Guide for Mapping Types of Information Systems to Security Categories, provides guidance for understanding the security objectives and impact levels identified in FIPS 199.

In accordance with FIPS 199 and NIST SP 800-60, a security categorization and analysis was performed for eOPF. The security categorization analysis of eOPF resulted in an overall security categorization of *high*.

OIG reviewed the eOPF FIPS 199 analysis and agreed with the "high" categorization of the system.

VIII. NIST 800-53 Evaluation

NIST SP 800-53 provides guidance for implementing a variety of security controls for information systems supporting the Federal government. These controls are organized into three classes (management, operational, and technical). The OIG tested a subset of these controls for eOPF as part of this audit, including:

- AC-7: Unsuccessful Login Attempts
- AC-10: Concurrent Session Control
- AC-11: Session Lock
- AC-15: Automated marking
- AU-2: Auditable Events
- AU-6: Audit Monitoring
- CM-2: Configuration Change Control
- CP-4: Contingency Plan Testing
- IA-5: Authenticator Management
- IR-2: Incident Response Training
- IR-5: Incident Monitoring
- PL-3: System Security Plan Update
- PL-4: Rules of Behavior
- RA-5: Vulnerability Scanning
- SA-3: Life Cycle Support

The OIG determined whether these controls were in place by interviewing individuals with eOPF security responsibilities, reviewing documentation and system screenshots provided by HRLOB, and conducting tests directly on the system.

We determined that HRLOB was generally compliant with NIST SP 800-53 guidance by implementing the appropriate security controls for eOPF. However, control IA-5, Authenticator Management, was not fully implemented when the OIG reviewed this control in February 2009. At that time, eOPF was not configured to periodically force

users to change their password. During the fieldwork phase of this audit, eOPF was re-configured to force password changes every 90 days, and control IA-5 is now satisfied.

Although the OIG determined that six additional controls have not been implemented for this system, the weaknesses had been previously identified by HRLOB and were appropriately added as action items to the eOPF plan of action and milestones (POA&M). Five of the six remaining control weaknesses were scheduled to be addressed in 2009. However, the eOPF POA&M states that corrective actions for control [redacted] are over 120 days overdue, and should be considered a high priority for HRLOB.

IX. Plan of Action and Milestones Process

A POA&M is a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for IT security weaknesses. OPM has implemented an agency-wide POA&M process to help track known IT security weaknesses associated with the agency's information systems.

HRLOB submitted a current POA&M to OPM's CIS in November 2008. The OIG evaluated the following aspects of this POA&M:

Prioritization of Weaknesses

HRLOB uses the POA&M template provided by OPM's CIS to track security control weaknesses of eOPF. This template facilitates the prioritization of POA&M weaknesses, and HRLOB appears to be prioritizing its weaknesses per OPM policy and FISMA requirements.

Proof of Closure

The eOPF POA&M indicates that several security weaknesses were recently closed. OIG requested evidence of the "proof of closure" documentation that was submitted to OPM's CIS/CIO at the time the POA&M item was closed. We requested proof of closure for seven control weaknesses that were identified on the POA&M as closed between April and October, 2008. The OIG was provided with adequate proof of closure documentation for all seven requested items.

Including All Identified Weaknesses in POA&M

A test of eOPF security controls was conducted in July 2008 by an independent company, Carson Associates, contracted to conduct the test. The test included a review of the management, operational, and technical security controls outlined in NIST SP 800-53. Carson Associates identified multiple instances in which eOPF's controls did not satisfy the requirements of NIST SP 800-53. The OIG verified that each of the weaknesses identified by Carson Associates was included on the eOPF POA&M.

The OIG is not aware of any other recent security assessments of eOPF that could lead to the identification of potential POA&M items.

Nothing came to our attention during the review of the eOPF POA&M to indicate that HRLOB needs to improve its POA&M management process.

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

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of Modernization
and Human Resources
Line of Business

MEMORANDUM FOR [redacted]
Chief, Information Systems Audits Group

FROM: [redacted]
Program Director, Enterprise Human Resources Integration
Human Resources Line of Business

Subject: Program Office Response to OIG Report Number 4A-HR-00-09-032, "Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Electronic Official Personnel Folder"

Thank you for the opportunity to comment on the Office of the Inspector General (OIG) Draft Report, "Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Electronic Official Personnel Folder."

The Human Resources Line of Business (HRLOB) Enterprise Human Resources Integration (EHRI) Program Office has reviewed the report and agrees with the findings, conclusions, and recommendations presented. The Program Office is committed to resolving all outstanding IT security-related issues in a timely manner and greatly appreciates the feedback provided by the OIG as part of its evaluation.

cc: [redacted]
Deputy Associate Director
Center for Information Services and Chief Information Officer

[redacted]
Information Technology Specialist
Center for Information Services

[redacted]
Deputy Chief Financial Officer

[redacted]
Human Resources Line of Business