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 PRESIDENTIAL MANAGEMENT FELLOWS SYSTEM FY 2011

Report No. 4A-HR-00-11-017

Date: May 16, 2011

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 PRESIDENTIAL MANAGEMENT FELLOWS SYSTEM FY 2011

WASHINGTON, D.C.

Report No. 4A-HR-00-11-017

Date: 5/16/2011

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 PRESIDENTIAL MANAGEMENT FELLOWS SYSTEM FY 2011

WASHINGTON, D.C.

Report No. 4A-HR-00-11-017

Date: 5/16/2011

This final audit report discusses the results of the Office of the Inspector General's (OIG) review of the information technology security controls of the U.S. Office of Personnel Management's (OPM) Presidential Management Fellows System (PMF). Our conclusions are detailed in the "Results" section of this report.

We determined that the following elements of the PMF security program appear to be in full compliance with the Federal Information Security Management Act:

- A security certification and accreditation of PMF was completed in October 2009.
- We agree with the security categorization of "moderate" for PMF.
- The PMF Information System Security Plan (ISSP) contains the necessary requirements defined by NIST SP 800-18 Revision 1.
- A Security Test and Evaluation (ST&E) was completed for PMF in September 2009.
- The PMF security controls self assessment was conducted for the FY 2011.
- A contingency plan was completed and tested for the PMF System in 2010.

- A risk assessment was conducted for PMF in 2010 that addresses all the required elements outlined in relevant guidance.
- The PMF Plan of Action and Milestones (POA&M) follows the format of the OPM POA&M guide, and has been routinely submitted to the Office of the Chief Information Officer for evaluation.

During the initial field work phase of the audit the OIG documented the following opportunities for improvement:

- The PMF Privacy Impact Assessment (PIA) was missing several elements required by the Office of Management and Budget.
- Employee Services (ES) did not have a formal process that requires agency coordinators to actively audit the user accounts they have created.
- New users of the PMF system are sent an automated e-mail stating the password requirements to follow when creating their accounts. However, the requirements outlined in the email did not match the actual system settings.

Between the issuance of the draft report and this final report, ES has taken the following actions to correct the items listed above:

- On January 12, 2011 a new PIA for PMF was completed which adheres to OPM's updated PIA Guide.
- ES implemented a process that requires all agency coordinators to review active user accounts on a semi-annual basis and notify the program office of any accounts that should be disabled.
- The automated email sent to new users was revised to accurately reflect PMF password requirements.

After reviewing the supporting documentation provided by ES we have determined that the initial audit concerns have been addressed and no further action is required.

Contents

Introduction

On December 17, 2002, President Bush 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) Presidential Management Fellows System (PMF).

Background

PMF is one of OPM's 43 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 PMF website provides potential PMF candidates, Federal agencies, and OPM staff with information about the PMF program. The PMF system is also used by federal agencies and Fellows candidates to facilitate the fellowship selection process.

OPM's Employee Services (ES) division has ownership and managerial responsibility of the PMF system. ES contracts with OPM's Human Resources Tools and Technology group (HRTT) within the Human Resources Solutions division to provide the software development, maintenance, application hosting, operations, and security of this system.

Objectives

Our objective was to perform an evaluation of the security controls for the PMF to ensure that ES and HRTT officials have implemented IT security policies and procedures in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), and OPM's Office of the Chief Information Officer (OCIO).

OPM's IT security policies require managers of all major information 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 audit objective was accomplished by reviewing the degree to which a variety of security program elements have been implemented for PMF, including:

- Certification and Accreditation Statement;
- FIPS 199 Analysis;
- Information System Security Plan;
- Risk Assessment;
- Independent Security Control Testing;
- Security Control Self-Assessment;
- Contingency Planning and Contingency Plan Testing;

- Privacy Impact Assessment;
- Plan of Action and Milestones Process; and
- NIST Special Publication (SP) 800-53 Security Controls.

Scope and Methodology

This 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 ES and HRTT officials responsible for PMF, including IT security controls in place as of January 2011.

We considered the PMF 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 ES division and other individuals with PMF 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 PMF 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 PMF system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Technology Security Policy Volumes 1 and 2;
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- 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 3, 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 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 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 November 2010 through January 2011 in OPM's Washington, D.C. office. This was our first audit of the security controls surrounding PMF.

Compliance with Laws and Regulations

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

Results

I. Certification and Accreditation Statement

A security certification and accreditation (C&A) of PMF was completed in October 2009.

NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems," provides guidance to federal agencies in meeting security accreditation requirements. The PMF C&A appears to have been conducted in compliance with NIST requirements.

OPM's Senior Agency Information Security Officer (representing the Office of the Chief Information Officer or OCIO) reviewed the PMF C&A package and signed the system's certification package on October 8, 2009. The system's owner (OPM's Associate Director of Human Resources) signed the accreditation statement and authorized the continued operation of the system on October 13, 2009.

II. FIPS 199 Analysis

Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, requires federal agencies to categorize all federal information and information systems in order to provide appropriate levels of information security according to a range of risk levels.

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

The PMF information system security plan (ISSP) categorizes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. PMF is categorized with a moderate impact level for confidentiality, moderate for integrity, low for availability, and an overall categorization of moderate.

The security categorization of PMF appears to be consistent with FIPS 199 and NIST SP 800-60 requirements, and the OIG agrees with the categorization of moderate.

III. Information System Security Plan

Federal agencies must implement on each information system the security controls outlined in NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems. NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in an ISSP for each system, and provides guidance for doing so.

The ISSP for PMF was created using the template outlined in NIST SP 800-18 Revision 1. The template requires that the following elements be documented within the ISSP:

- System Name and Identifier;
- System Categorization;
- System Owner;
- Authorizing Official;
- Other Designated Contacts;
- Assignment of Security Responsibility;
- System Operational Status;
- Information System Type;
- General Description/Purpose;
- System Environment;
- System Interconnection/Information Sharing;
- Laws, Regulations, and Policies Affecting the System;
- Security Control Selection;
- Minimum Security Controls; and
- Completion and Approval Dates.

The PMF ISSP adequately addresses each of the elements required by NIST.

IV. Risk Assessment

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 SP 800-30, Risk Management Guide for Information Technology Systems, 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.

A risk assessment was conducted for PMF in 2010 that adequately addresses all of the elements outlined in the NIST guidance.

V. Independent Security Control Testing

A security test and evaluation (ST&E) was completed for PMF in September 2009 as a part of the system's C&A. The ST&E was conducted by a contractor, Capricorn Systems Inc., which was operating independently from ES and HRTT. The OIG reviewed the controls tested to ensure that they included a review of the appropriate management, operational, and technical controls required for a system with a "moderate" security categorization according to NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

The ST&E report labeled each security control as fully satisfied, partially satisfied, not satisfied, not verified, or not applicable. Several controls were also identified as "common controls" inherited from OPM's general support and infrastructure systems. Nothing came to our attention to indicate that the security controls of PMF have not been adequately tested by an independent source.

VI. Security Control Self-Assessment

FISMA requires that the IT security controls of each major application owned by a federal agency be tested on an annual basis. In the years that an independent ST&E is not being conducted on a system, the system's owner must conduct an internal self-assessment of security controls.

The designated security officer for PMF conducted a self-assessment of the system in September 2010. The assessment included a review of the relevant management, operational, and technical security controls outlined in NIST SP 800-53. Nothing came to our attention to indicate that the security controls of PMF have not been adequately tested by ES and HRTT.

VII. Contingency Planning and Contingency Plan Testing

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. OPM's security policies require all major applications to have viable and logical disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

Contingency Plan

The PMF contingency plan documents the functions, operations, and resources necessary to restore and resume PMF operations when unexpected events or disasters occur. The PMF contingency plan closely follows the format suggested by NIST SP 800-34 and contains a majority of the required elements.

Contingency Plan Test

NIST SP 800-34, Contingency Planning Guide for Information Technology, provides guidance for testing contingency plans and documenting the results. Contingency plan testing is a critical element of a viable disaster recovery capability.

A simulated "table top" test of the PMF contingency plan was conducted by ES and HRTT officials in April 2010. We reviewed the testing documentation to determine if the test conformed with NIST 800-34 guidelines. The simulation test involved reviewing a series of steps that must be completed to recover the system in a disaster situation. The testing documentation contained an analysis and review of the simulation

results. Nothing came to our attention to indicate that the PMF contingency plan has not been adequately tested.

VIII. Privacy Impact Assessment

The E-Government Act of 2002 requires agencies to perform a screening of federal information systems to determine if a Privacy Impact Assessment (PIA) is required for that system. OMB Memorandum M-03-22 outlines the necessary components of a PIA. The purpose of the assessment is to evaluate any vulnerabilities of privacy in information systems and to document any privacy issues that have been identified and addressed.

ES and HRTT completed an initial privacy screening of the PMF system and determined that a PIA was required for this system. In September of 2009, a PIA was completed for this system based on the guidelines contained in OPM's PIA Guide.

However, OPM's PIA Guide was missing several elements required by OMB. Consequently, the PIA for PMF is missing these elements as well. OPM has recently updated its PIA Guide to meet OMB requirements, and the OCIO's Security and Privacy Group is working with program offices to complete a new PIA for each system.

Recommendation 1

We recommend that ES conduct a PIA for PMF based on the updated PIA Guide.

ES Response:

"During the audit, it was reported that OPM's PIA Guide was not updated to reflect newer OMB required elements. OPM's OCIO's Security and Privacy Group recently updated OPM's PIA Guide and is working with program offices to complete a new PIA. The last time the PIA was updated for the PMF System was in September 2009.

On January 12, 2011, a new PIA on the PMF System was completed which adheres to OPM's updated PIA Guide. [ES] signed the new PIA, as the System Owner, and it was submitted to OCIO ([redacted] for their approval on January 13, 2011. On January 19, 2011, [ES] received a confirmation email from [redacted] stating Matt Perry, OPM's Chief Privacy Officer, signed the PIA. On January 20, 2011, [ES] received a signed copy of the PIA from OCIO. We believe this action should satisfy and close the finding."

OIG Reply:

We have reviewed the updated PIA for PMF and determined it now meets all OMB requirements; no further action is required.

IX. 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 OIG evaluated the PMF POA&M and verified that it follows the format of OPM's standard template, and has been routinely submitted to the OCIO for evaluation. We also determined that the POA&M contained action items for all security weaknesses identified through various security control tests and audits.

Nothing came to our attention to indicate that there are any current weaknesses in the management of the PMF POA&M.

X. NIST SP 800-53 Evaluation

NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems, provides guidance for implementing a variety of security controls for information systems supporting the federal government. As part of this audit, we evaluated the degree to which a subset of these controls had been implemented for PMF, including:

- AC-2 Account Management
- AC-6 Least Privilege
- AC-7 Unsuccessful Login Attempts
- AC-8 System Use Notification
- AC-11 Session Lock
- AC-13 Supervision and Review – Access Control
- AC-22 Publicly Accessible Information
- AT-3 Security Training
- AU-2 Auditable Events
- AU-6 Audit Review, Analysis, Reporting
- AU-9 Protection of Audit Information
- CM-2 Baseline Configuration
- IA-2 Identification and Authentication
- IA-5 Authenticator Management
- IA-8 Identification and Authentication (Non-organizational users)
- PL-4 Rules of Behavior
- PS-4 Personnel Termination
- RA-5 Vulnerability Scanning
- SC-2 Application Partitioning
- SC-8 Transmission Integrity

These controls were evaluated by interviewing individuals with PMF security responsibilities, reviewing documentation and system screenshots, viewing demonstrations of system capabilities, and conducting tests directly on the system.

Although it appears that the majority of NIST SP 800-53 security controls have been successfully implemented for the PMF, several tested controls were not fully satisfied.

a) AC-2 Account Management / PS-4 Personnel Termination

The PMF system has users internal to OPM as well as users at other federal agencies that participate in the PMF program. Each of these external agencies has an "agency coordinator" that is responsible for creating and removing PMF user accounts at their

respective agencies. Although ES has adequate controls to remove access for OPM users when necessary, the security controls related to the accounts created by agency coordinators could be improved.

[redacted]

NIST SP 800-53 Control AC-2 requires an organization to review, disable, and remove user accounts when necessary. Control PS-4 states that an organization must remove a user's information system access immediately upon the individual's termination of employment.

[redacted]

Recommendation 2

We recommend ES routinely provide external agencies [redacted], and request that each [redacted]

ES Response:

"An [redacted] has been created and is accessible via PMF Administrator. We are now able to [redacted] A sample of this new report is attached for your reference.

The PMF Program Office will require [redacted] We believe this action should satisfy and close the finding."

OIG Reply:

We have reviewed the supporting documentation provided by ES and determined that this audit recommendation has been adequately addressed; no further action is required.

b) IA-5 Authenticator Management

New users to the PMF system are sent an automated email with a username and temporary password to access the system. Users are forced to change their password

immediately after their initial log in. The automated email states that the new password must meet the following criteria:

However, [redacted] outlines a different set of password criteria:

Upon testing the password requirements, we determined that the password criteria outlined in the automated email is not accurately enforced, as the system required the password to [redacted] The password criteria outlined on [redacted] appears to be accurate.

NIST 800-53 Control IA-5 requires an organization to establish a control to authenticate a user when logging into the system, and that the organization develops a formal set of rules for passwords.

Recommendation 3

We recommend that ES and HRTT verify the technical implementation of PMF password requirements and make the appropriate updates to the password policies outlined in the automated new user email and [redacted]

ES Response:

"During the OIG audit, it was discovered that the automated new user email containing password requirements was not consistent with the instructions on password requirements found [redacted] In coordination with HRTT, the text of the automated new user email was updated to match password requirements for consistency. A copy of the revised automated new user email, highlighting the updated password requirements, is attached for your reference. We believe this action should satisfy and close the finding."

OIG Reply:

We have reviewed the supporting documentation provided by ES and determined that this audit recommendation has been adequately addressed; no further action is required.

Major Contributors to this Report

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

- [redacted], Group Chief
- [redacted], Senior Team Leader
- [redacted], IT Auditor