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 PERSONNEL INVESTIGATIONS PROCESSING SYSTEM FY 2013

Report No. 4A-IS-00-13-022

Date: June 24, 2013

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S PERSONNEL INVESTIGATIONS PROCESSING SYSTEM FY 2013

WASHINGTON, D.C.

Report No. 4A-IS-00-13-022

Date: June 24, 2013

Michael R. Esser
Assistant Inspector General for Audits

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S PERSONNEL INVESTIGATIONS PROCESSING SYSTEM FY 2013

WASHINGTON, D.C.

Report No. 4A-IS-00-13-022

Date: June 24, 2013

This final audit report discusses the results of our audit of the information technology security controls of the U.S. Office of Personnel Management's (OPM) Personnel Investigations Processing System (PIPS). Our conclusions are detailed in the "Results" section of this report.

Security Assessment and Authorization (SA&A)

An SA&A of PIPS was completed in June 2011. We reviewed the authorization package for all required elements of an SA&A, and determined that the package contained all necessary documentation.

Federal Information Processing Standards (FIPS) 199 Analysis

The security categorization of PIPS appears to be consistent with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 requirements, and we agree with the categorization of "high."

System Security Plan (SSP)

The PIPS SSP contains the critical elements required by NIST SP 800-18. However, several controls listed in the SSP as common or inherited are inappropriately labeled.

Risk Assessment

A risk assessment was conducted for PIPS as a part of their 2011 SA&A. All major elements outlined in the NIST guidance were addressed.

Independent Security Control Testing

A security control assessment was completed for PIPS in April 2011 as a part of the system's SA&A process. As a result of the inappropriately labeled controls in the SSP, the Bureau of Public Debt inappropriately removed these controls from its security control test plan, and these controls have not been adequately tested.

Security Control Self-Assessment

Federal Investigative Services implemented an Information Security Continuous Monitoring Plan that addresses the annual self-assessment requirements. However, the security plan inappropriately labels several controls as common or inherited, thus impacting the ability of FIS to appropriately implement and test the PIPS controls.

Contingency Planning and Contingency Plan Testing

A contingency plan was developed for PIPS that is in compliance with NIST SP 800-34 and is tested annually.

Privacy Impact Assessment (PIA)

A privacy threshold analysis was conducted for PIPS and indicated that a PIA was required. A PIA was conducted in June 2011.

Plan of Action and Milestones (POA&M) Process

The PIPS POA&M is routinely submitted to the Office of the Chief Information Officer for evaluation and generally follows the format of the OPM POA&M guide, with a few exceptions regarding the level of detail required by the OPM guide. However, there are a substantial number of significantly over due POA&M items.

NIST SP 800-53 Evaluation

We evaluated the degree to which a subset of the IT security controls outlined in NIST SP 800-53 Revision 3 was implemented for PIPS and found no issues beyond those previously identified.

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 audited the information technology (IT) security controls related to the Office of Personnel Management's (OPM) Personnel Investigations Processing System (PIPS).

Background

OPM's Federal Investigative Services (FIS) has ownership of PIPS. PIPS is utilized to process hundreds of thousands of background investigations each year. The system contains the OPM Security/Suitability Investigations Index and maintains approximately 15 million records of investigations conducted by and for OPM, the Federal Bureau of Investigations, the U.S. Department of State, the Secret Service, and other customer agencies. The PIPS system interfaces with several other FIS systems to process applications and the flow of data relies on both the OPM Local Area Network / Wide Area Network (LAN/WAN) and Enterprise Server Infrastructure (ESI) general support systems. As a function of oversight, the Office of the Chief Information Officer (OCIO) assigned an Information System Security Officer (ISSO) to manage a variety of security functions on behalf of FIS.

Objectives

Our objective was to perform an evaluation of the security controls for PIPS to ensure that FIS has implemented IT security policies and procedures in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual (FISCAM), and OPM's 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 PIPS, including:

- Security Assessment and Authorization;
- FIPS 199 Analysis;
- 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 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 FIS, including IT security controls in place as of January 2013.

We considered the PIPS 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 objectives, we interviewed representatives of OPM with security responsibilities for PIPS. 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 PIPS 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 PIPS system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Security and Privacy Policy Handbook;
- 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;
- The Federal Information System Controls Audit Manual;
- 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;
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities;

- Federal Information Processing Standards Publication (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 November 2012 through January 2013 in OPM's Washington, D.C. office. This was our first audit of the security controls surrounding PIPS.

Compliance with Laws and Regulations

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

Results

I. Security Assessment and Authorization

A Security Assessment and Authorization (SA&A) of PIPS was completed in June 2011.

OPM's Chief Information Security Officer reviewed the PIPS SA&A package and signed the system's authorization letter on July 19, 2011. The system's authorizing official signed the letter and authorized the continued operation of the system on July 24, 2011.

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 PIPS SA&A appears to have been conducted in compliance with NIST requirements.

II. FIPS 199 Analysis

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 PIPS FIPS 199 categorizes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. PIPS is categorized with a high impact level for confidentiality and integrity and moderate for availability, resulting in an overall categorization of high.

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

III. System Security Plan

Federal agencies must implement on each information system the security controls outlined in NIST SP 800-53 Revision 3, 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 a System Security Plan (SSP) for each system, and provides guidance for doing so.

The SSP for PIPS was created using a template that is outlined in the OPM SSP guide. The SSP contains the majority of the elements outlined in NIST SP 800-18. However, during the review of controls listed in the SSP as common or inherited it was determined that several were inappropriately labeled. NIST 800-18 explains that common or inherited controls are "those controls covered at the agency level, which are not system-specific." (9) NIST also defines a common security control as having "the following properties: (i) the development,

implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied." Labeling controls incorrectly as common/inherited increases the likelihood that controls are not properly implemented at the system level, which in turn increases the risk that individuals can inappropriately access sensitive PIPS data.

Recommendation 1

We recommend that the PIPS ISSO, FIS, and the owners of the LAN/WAN and ESI, collaborate to ensure that all controls listed on the PIPS SSP are appropriately categorized as common, inherited, hybrid, or system specific.

FIS Response:

"FIS agrees with the recommendation to collaborate with the owners of LAN/WAN and ESI to ensure all security controls are appropriately categorized. FIS does note that the controls found within the Common Security Controls Collection (CSCC) are assessed and validated by the Information Technology Security and Privacy (ITSP) for insertion into this library for use amongst the various OPM systems as agency common controls. FIS intends to meet with the LAN/WAN and ESI owners to come to a mutual agreement on the control type and status for each control currently labeled as belonging to a control provider."

OIG Reply:

As part of the audit resolution process for this recommendation and all subsequent recommendations to which FIS agrees, please provide OPM's Internal Oversight and Compliance (IOC) division with evidence supporting the corrective action taken.

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 PIPS as a part of their 2011 SA&A. All major elements outlined in the NIST guidance were addressed.

V. Independent Security Control Testing

A security control assessment was completed for PIPS in April 2011 as a part of the system's SA&A process. The security assessment was conducted by another government agency, the Bureau of Public Debt (BPD). We reviewed the documentation resulting from this test to ensure that it 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, Recommended Security Controls for Federal Information Systems.

The BPD appeared to adequately test the security controls that were within the scope of this engagement. However, as mentioned in section III, above, the PIPS SSP incorrectly identified several controls as common or inherited. As a result, the BPD inappropriately removed these controls from its security control test plan, and these controls have not been adequately tested. Prior to the next independent test of security controls, an appropriately categorized list of security controls should be finalized as a result of Recommendation 1, above.

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 security assessment is not being conducted on a system, the system's owner must conduct an internal self-assessment of security controls. Furthermore, NIST SP 800-53 mandates the development of a security assessment plan and outlines the required inclusions.

On October 1, 2012, FIS implemented an Information Security Continuous Monitoring (ISCM) Plan that outlined an approach for testing all high volatility controls at a frequency no less than quarterly and moderate/low volatility controls at a frequency no less than annually. However, as mentioned in section III above, the FIS security plan inappropriately labels several controls as common or inherited. The current ISCM cannot be fully implemented until FIS identifies exactly which security controls are system specific and need to be subject to continuous monitoring.

Failure to complete an appropriately scoped security controls test increases the risk that IT security weaknesses are undetected and that FIS is unable to make informed judgments to appropriately mitigate risks to an acceptable level.

Recommendation 2

We recommend that, after all controls on the SSP have been reviewed and appropriately categorized, FIS ensure that a thorough test of security controls is completed for PIPS.

FIS Response:

"FIS agrees with the recommendation. Recognizing the concern identified by OIG with possible improperly categorized security controls within the SSP, FIS will fully review all security controls currently categorized as common or inherited and validate their accuracy while collaborating with the control provider. FIS will update the SSP accordingly based on this review, will include those found to be improperly categorized

into the current ISCM plan and will re-test all security controls during the next Assessment & Authorization cycle for PIPS (June 2014)."

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

Contingency Plan Test

NIST SP 800-34 also provides guidance for testing contingency plans and documenting the results. In addition, NIST SP 800-53 Control CP-3 requires system owners to "train personnel in their contingency roles and responsibilities with respect to the information system and provide refresher training."

FIS conducted a test of the system's contingency plan in 2012. The testing documentation includes the majority of elements suggested by NIST SP 800-83.

VIII. Privacy Impact Assessment

FISMA 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. The OPM Privacy Impact Assessment Guide states that all OPM IT systems must have a Privacy Threshold Analysis (PTA) which is utilized to determine if a PIA is required.

FIS completed a PTA of PIPS and determined that a PIA was required for this system. As such, a PIA was completed in June of 2011 based on the guidelines contained in OPM's PIA Guide.

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 PIPS POA&M and verified that it generally follows the format of OPM's standard template, and that updates are routinely submitted to OCIO for evaluation. However, the POA&M process is not being utilized effectively. The PIPS POA&M contained 21 security weaknesses, 4 of which have remediation activities in excess of 365 days overdue and an additional 17 remediation activities in excess of 120 days overdue. In addition, the PIPS POA&M contains the following inconsistences with OPM's POA&M Guide:

- The OPM POA&M color scheme is not being properly utilized to address delayed and late items;
- The "weakness" column for a significant number of items is missing the corresponding NIST guidance associated with the identified weakness;
- The "estimated completion date" column is not being utilized appropriately to track remediation efforts; and,
- The "comments" column is not being properly utilized to track the mitigation efforts for weaknesses and explain delayed items.

Failure to appropriately use the POA&M processes to address known security weaknesses in a timely manner increases the risk that someone could gain unauthorized access to the system or the data it contains.

Recommendation 3

We recommend that FIS develop a detailed action plan for the remediation of all overdue POA&M items.

FIS Response:

"FIS has, and will continue to provide a Corrective Action Plan (CAP) to OPM CIO ITSP, which describes the prioritization of resources (personnel and funding) to resolve all POAMs over 120 days. The PIPS CAP is reviewed and updated each quarter and provided to OPM CIO ITSP.

FIS agrees to provide more detail in the POAM and/or POAM Milestones and will reflect the specific detail appropriately into Trusted Agent FISMA (TAF)."

Recommendation 4

We recommend that FIS revise its existing POA&M items to include the required level of detail as explained in the OPM POA&M Guide.

FIS Response:

"FIS agrees with the need to increase the level of detail found within the existing POAMs. It has been noted that the current OPM POAM Guide is a bit outdated (September 2009) and it does not accurately reflect the current business process creation, monitoring, updating and closure of POA&Ms using the TAF application. FIS would request validation [that] the OPM POAM Guide has not changed the definition of "required level of detail" since original publication."

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 whether a subset of these controls had been implemented for PIPS. During our review of the POA&M process, we noted 21 open items which correspond to security controls that are not fully implemented for PIPS. In addition, we independently tested several security controls outlined in NIST SP 800-53 Revision 3 that are applicable to a FIPS 199 "high" categorized system. These controls were evaluated by interviewing individuals with PIPS security responsibilities, reviewing documentation and system screenshots, and viewing demonstrations of system capabilities.

Our testing did not identify any additional issues beyond those already noted on the PIPS POA&M.

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], Deputy Assistant Inspector General for Audits
- [redacted], Senior Team Leader
- [redacted], Auditor-in-Charge
- [redacted], IT Auditor

United States Office of Personnel Management

TO: [redacted]
Chief, Information Systems Audit Group
Office of Personnel Management

FROM: [redacted]
PIPS System Owne[redacted]
Office of Personnel
Federal Investigative Services (FIS)

4/25/2013

SUBJECT: **Response to "Draft" FY2013 FISMA System Audit of PIPS**

OIG Recommendation 1:
We recommend that the PIPS ISSO, FIS, and the owners of the LAN/WAN and ESI, collaborate to ensure that all controls listed on the PIPS SSP are appropriately categorized as common, inherited, hybrid, or system specific.

FIS Response:
FIS agrees with the recommendation to collaborate with the owners of LAN/WAN and ESI to ensure all security controls are appropriately categorized. FIS does note that the controls found within the Common Security Controls Collection (CSCC) are assessed and validated by the Information Technology Security and Privacy (ITSP) for insertion into this library for use amongst the various OPM systems as agency common controls. FIS intends to meet with the with the LAN/WAN and ESI owners to come to a mutual agreement on the control type and status for each control currently labeled as belonging to a control provider.

OIG Recommendation 2:
We recommend that, after all controls on the SSP have been reviewed and appropriately categorized, FIS ensure that a through test of security controls is completed for PIPS.

FIS Response:
FIS agrees with the recommendation. Recognizing the concern identified by OIG with possible improperly categorized security controls within the SSP, FIS will fully review all security controls currently categorized as common or inherited and validate their accuracy while collaborating with the control provider. FIS will update the SSP accordingly based on this review, will include those found to be improperly categorized into the current ISCM plan and will re-test all security controls during the next Assessment & Authorization cycle for PIPS (June 2014).

OIG Recommendation 3:
We recommend that FIS develop a detailed action plan for the remediation of all overdue POAM items

FIS Response:
FIS has, and will continue to provide a Corrective Action Plan (CAP) to OPM CIO ITSP, which describes the prioritization of resources (personnel and funding) to resolve all POAMs over 120 days. The PIPS CAP is reviewed and updated each quarter and provided to OPM CIO ITSP.

FIS agrees to provide more detail in the POAM and/or POAM Milestones and will reflect the specific detail appropriately into Trusted Agent FISMA (TAF).

OIG Recommendation 4:
We recommend that FIS revise its existing POAM items to include the required level of detail as explained in the OPM POAM Guide.

FIS Response:
FIS agrees with the need to increase the level of detail found within the existing POAMs. It has been noted that the current OPM POAM Guide is a bit outdated (September 2009) and it does not accurately reflect the current business process of creation, monitoring, updating and closure of POA&Ms using the TAF application. FIS would request validation the OPM POAM Guide has not changed the definition of "required level of detail" since original publication.