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

Final Audit Report

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's USA Performance System

Report Number 4A-HR-00-15-018
July 20, 2015

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's USA Performance System

Report No. 4A-HR-00-15-018 **July 20, 2015**

Why Did We Conduct the Audit?

The USA Performance (USAP) System is one of the U.S. Office of Personnel Management's (OPM) critical Information Technology (IT) systems. As such, the Federal Information Security Management Act (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.

What Did We Audit?

The OIG has completed a performance audit of USAP to ensure that the system owner, OPM's Human Resource Solutions (HRS) program office, has managed the implementation of IT security policies and procedures in accordance with the standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information Security Controls Audit Manual (FISCAM) and OPM's Office of the Chief Information Officer (OCIO).

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls of the USAP system determined that:

- A Security Assessment and Authorization (SA&A) of the USAP system was completed in June 2014. We reviewed the authorization package for all required elements of an SA&A, and determined that the package contained all necessary documentation.
- The security categorization of the USAP system is consistent with Federal Information Processing Standards 199 and NIST Special Publication (SP) 800-60 requirements, and we agree with the categorization of "moderate."
- The USAP System Security Plan contains the critical elements required by NIST SP 800-18 Revision 1.
- A security control assessment plan and report were completed in March and May 2014, respectively, for the USAP system.
- The HRS IT Program Management Office has performed regular security control self-assessments in accordance with OPM's continuous monitoring methodology.
- A contingency plan was developed for the USAP system that is in compliance with NIST SP 800-34 Revision 1, and the plan is tested annually.
- A Privacy Threshold Analysis was conducted for the USAP system that indicated that a Privacy Impact Assessment (PIA) was required. A PIA has been conducted, however the PIA has not been finalized and approved.
- The USAP system's Plan of Acton and Milestones (POA&M) follows the format of OPM's standard template and has been loaded into Trusted Agent, the OCIO's POA&M tracking tool.
- We evaluated the degree to which a subset of the IT security controls outlined in NIST SP 800-53 Revision 4 were implemented for the USAP system. We determined that the security controls selected for testing appear to be in compliance with NIST SP 800-53 Revision 4.

ABBREVIATIONS

FIPS	**Federal Information Processing Standards**
FISCAM	**Federal Information System Controls Audit Manual**
FISMA	**Federal Information Security Management Act**
GAO	**U.S. Government Accountability Office**
HRS	**Human Resources Solutions**
IG	**Inspector General**
IT	**Information Technology**
ITSP	**Information Technology Security and Privacy Group**
NIST	**National Institute of Standards and Technology**
OCIO	**Office of the Chief Information Officer**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
PIA	**Privacy Impact Analysis**
PMO	**Program Management Office**
POA&M	**Plan of Action & Milestones**
PTA	**Privacy Threshold Analysis**
SA&A	**Security Assessment & Authorization**
SAP	**Security Assessment Plan**
SAR	**Security Assessment Report**
SP	**Special Publication**
SSP	**System Security Plan**
USAP	**USA Performance**

TABLE OF CONTENTS

I. BACKGROUND

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 U.S. 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 U.S. Office of Personnel Management's (OPM) USA Performance (USAP) system.

The USAP system is one of OPM's 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 USAP system is a web-based application designed to assist Federal agencies in implementing their Senior Executive Service (SES) and Non-SES performance management program and systems. Agencies can develop performance plans, track and monitor employee's performance, provide feedback and ratings, and electronically sign off on performance plans.

OPM's Human Resource Solutions - Performance Management Solutions is the program office that owns the business processes supported by the USAP system. The Human Resources Solutions (HRS) Information Technology (IT) Program Management Office (PMO) is the organization responsible for the software development, maintenance, and technical operation of this system. The HRS IT organization is part of OPM's Office of the Chief Information Officer.

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

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objective

Our objective was to perform an evaluation of the system's security controls to ensure that USAP officials have managed the implementation of 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.

The audit objective was accomplished by reviewing the degree to which a variety of security program elements have been implemented for the USAP system, including:

- Security Assessment and Authorization (SA&A);
- Federal Information Processing Standards (FIPS) 199 Analysis;
- System Security Plan (SSP);
- Security Assessment Plan and Report (SAP) and (SAR);
- Security Control Self-Assessment;
- Contingency Planning and Contingency Plan Testing;
- Privacy Impact Assessment (PIA);
- Plan of Action and Milestones Process (POA&M); and
- NIST Special Publication (SP) 800-53 Revision 4 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 officials responsible for the USAP system, including IT security controls in place as of May 2015.

We considered the USAP system 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 OPM representatives with the USAP system security responsibilities, reviewed documentation and system screenshots, viewed demonstrations of system capabilities, and conducted tests directly on the system. We also 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 the USAP system are located in the "Audit Findings and Recommendations" 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 USAP 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 Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems;
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60 Revision 1, 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;
- 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 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 OIG, as established by the Inspector General Act of 1978, as amended. The audit was conducted from November 2014 through June 2015 in OPM's

Washington, D.C. office. This was our first audit of the security controls surrounding the USAP system.

Compliance with Laws and Regulations

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

II. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Assessment & Authorization

The SA&A of the USAP system was completed in June 2014.

OPM's Chief Information Security Officer and the system's authorizing official signed the system's authorization letter on June 26, 2014.

NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, provides guidance to federal agencies in meeting security accreditation requirements. The USAP system SA&A appears to have been conducted in compliance with NIST requirements.

B. 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 USAP system FIPS Publication 199 Security Categorization analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. The USAP system is categorized with a moderate impact level for confidentiality, moderate for integrity, moderate for availability, and an overall categorization of "moderate."

The security categorization of the USAP system appears to be consistent with FIPS Publication 199 and NIST SP 800-60 requirements, and we agree with the categorization of "moderate."

C. System Security Plan

Federal agencies must implement on each information system the security controls outlined in NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information systems and Organizations. 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 the USAP system was created using the OCIO's template that utilizes NIST SP 800-18 Revision 1 as guidance. The template requires that the following elements be documented within the SSP:

- 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.

We reviewed the USAP SSP and determined that it adequately addresses each of the elements required by NIST. Nothing came to our attention to indicate that the USAP system security plan has not been properly documented and approved.

D. Security Assessment Plan and Report

A Security Assessment Plan and a Security Assessment Report were completed for the USAP system in March 2014 and May 2014, respectively, as a part of the system's SA&A process. The SAP and SAR were completed by a contractor that was operating independently from OPM. We reviewed the documents to verify that a risk assessment was conducted in accordance with NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments. We also verified that appropriate management, operational, and technical controls were tested for a system with a "moderate" security categorization according to NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

The SAP outlined the assessment approach, scanning authorization, and test methods. The SAR identified 23 control weaknesses; based on review of supplemental evidence provided by OPM, the security assessment team was able to close all 23 findings. All weakness identified were classified with a low or medium risk rating.

We also reviewed the security assessment results table that contained the detailed results of the NIST SP 800-53 Revision 4 controls testing. The table confirmed that all 23 findings were closed as summarized in the SAR.

Nothing came to our attention to indicate that the security controls of the USAP system have not been adequately tested by an independent source.

E. Continuous Monitoring

OPM's Information Security and Privacy Handbook states that continuous monitoring security reports must be provided to the OCIO's Information Technology Security and Privacy Group (ITSP) at least semiannually. The OCIO also creates continuous monitoring plans each fiscal year that clearly describe the type and frequency of NIST SP 800-53 Revision 4 security controls that must be tested throughout the year.

In FY 2015, HRS IT PMO submitted evidence of the USAP system continuous monitoring security control testing to the ITSP in a timely manner.

Nothing came to our attention to indicate continuous monitoring activities related to the USAP system were not in compliance with OPM guidelines.

F. Contingency Planning and Contingency Plan Testing

NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information 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 USAP system contingency plan documents the functions, operations, and resources necessary to restore and resume the USAP system operations when unexpected events or disasters occur. The USAP system contingency plan adequately follows the format suggested by NIST SP 800-34 Revision 1 and contains the required elements.

Contingency Plan Test

NIST SP 800-34 Revision 1 provides guidance for testing contingency plans and documenting the results. Contingency plan testing is a critical element of a viable disaster recovery capability.

A contingency plan test of the USAP system contingency plan was conducted in April 2014. The test involved restoring data and application source code to new equipment. The testing documentation contained adequate analysis and review of the test results.

Nothing came to our attention to indicate the USAP system contingency plan has not been developed and tested in accordance with OPM policy.

G. Privacy Impact Assessment

FISMA requires agencies to perform a screening of federal information systems to determine if a 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.

The USAP program office completed an initial privacy screening or Privacy Threshold Analysis (PTA) of the USAP system and determined that a PIA is required for this system. A PIA was conducted during the systems SA&A and submitted to the Privacy Officer/ITSP for approval. However, the PIA for the USAP system has not yet been finalized and approved.

According to OPM policy, a PIA must be conducted when a PTA indicates that a PIA is required. Failure to conduct and approve a PIA increases the risk of sensitive data being disclosed.

Recommendation 1

We recommend that HRS and OCIO immediately finalize and obtain approval of the PIA for USAP in accordance with OPM policy.

HRS Response:

"in regards to 'Recommendation 1 … to finalize and obtain approval of the Privacy Impact Assessment,' a PIA was conducted during the USA Performance System Security Assessment and Authorization (SA&A), but was not approved at the time of the audit. The PIA is being finalized by the Information Technology Security and Privacy Group and should be approved shortly"

OIG Reply:

As part of the audit resolution process, HRS should provide evidence that the PIA has been approved by OPM's Office of Internal Oversight and Compliance.

H. 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.

We evaluated the USAP system POA&M and verified that it follows the format of OPM's standard template and has been loaded into Trusted Agent, the OCIO's POA&M tracking tool, for evaluation. Nothing came to our attention to indicate that there are any current weaknesses with the management of POA&Ms.

I. NIST SP 800-53 Evaluation

NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, 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 the USAP system. We evaluated approximately 45 security controls outlined in NIST SP 800-53 Revision 4 that were identified as being system specific or a hybrid control. Controls identified as common or inherited were omitted from testing because another system or program office is responsible for implementing the control. We tested one or more controls from each of the following control families:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Risk Assessment
- System Services and Acquisition
- System and Communications Protection
- System and Information Integrity

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

We determined that all tested security controls appear to be in compliance with NIST SP 800-53 Revision 4 requirements with the exception of the Privacy Impact Assessment issue identified in section G, above.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], Auditor-In-Charge
[redacted], IT Auditor

[redacted], Group Chief

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Human Resources
Solutions

May 22, 2015

MEMORANDUM FOR [redacted]
Chief, Information Systems Audit Group
Office of the Inspector General

FROM: JOSEPH S. KENNEDY
Associate Director, Human Resources Solutions
USA Performance Authorizing Official

SUBJECT: Response to Draft Report "Audit of the Info1mation Technology Security Controls of the OPM's USA Performance System (Report No. 4A-HR-00-15-018)"

The OPM USA Performance Program Office acknowledges and appreciates the work of the Office of Inspector General to evaluate the USA Performance System's compliance with the Federal Information Security Management Act (FISMA). This memorandum serves as an official response to the draft report.

The audit had no major findings. However, in regards to "Recommendation 1 … to finalize and obtain approval of the Privacy Impact Assessment," a PIA was conducted during the USA Performance System Security Assessment and Authorization (SA&A), but was not approved at the time of the audit. The PIA is being finalized by the Information Technology Security and Privacy Group and should be approved shortly.

HRS concurs with the audit outcome and has no other official comments.

cc:

Donna Seymour
Chief Information Officer

Janet Barnes
Director
Internal Oversight and Compliance

[redacted]
Senior Agency Information Security Officer
Office of the Chief Information Officer

[redacted]

USA Performance Program Manager
HR Solutions

[redacted]
Manager, Human Resources Solutions IT Program Management Office
Federal IT Business Solutions
Office of the Chief Information Officer

Paul Craven
Association CIO, Federal IT Business Solutions
Office of the Chief Information Officer

[redacted]
Software Quality Assurance Branch
Human Resources Solutions IT Program Management Office
Office of the Chief Information Officer

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone:

Toll Free Number:	(877) 499-7295
Washington Metro Area:	(202) 606-2423

By Mail:

Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100