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 USA STAFFING SYSTEM FY 2013

Report No. 4A-HR-00-13-024

Date: June 21, 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 USA STAFFING SYSTEM FY 2013

WASHINGTON, D.C.

Report No. 4A-HR-00-13-024

Date: June 21, 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 USA STAFFING SYSTEM FY 2013

WASHINGTON, D.C.

Report No. 4A-HR-00-13-024

Date: June 21, 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) USA Staffing System (USAS). Our conclusions are detailed in the "Results" section of this report.

Security Assessment and Authorization (SA&A)

An SA&A of USAS was completed in July 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 USAS 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 "moderate."

System Security Plan (SSP)

The USAS SSP contains the critical elements required by NIST SP 800-18.

Security Assessment Plan and Report

A security control assessment plan and report were completed for USAS as a part of the system's SA&A process in July 2011.

Security Control Self-Assessment

Human Resources Tools and Technology (HRTT) conducted a self-assessment of the security controls of USAS in August 2012.

Contingency Planning and Contingency Plan Testing

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

Privacy Impact Assessment (PIA)

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

Plan of Action and Milestones (POA&M) Process

The USAS POA&M follows the format of the OPM POA&M guide, and has been routinely submitted to the OCIO for evaluation.

NIST SP 800-53 Revision 3 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 USAS. Every security control that we tested has been adequately implemented.

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) USA Staffing System (USAS).

Background

USAS 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 USAS web-based application is a single integrated software solution, which enables Human Resource Management (HRM) personnel to design custom assessment tools, job application questionnaires, and job vacancy announcements for filling Government jobs. The system is operated and hosted by the Office of the Chief Information Officer, Human Resources Tools and Technology (HRTT).

This was our first audit of the security controls surrounding USAS. We discussed the results of our audit with HRS and HRTT representatives at an exit conference.

Objectives

Our objective was to perform an evaluation of the security controls for USAS to ensure that HRTT officials have 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 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 USAS, including:

- Security Assessment and Authorization;
- FIPS 199 Analysis;
- System Security Plan;
- Security Assessment Plan and Report;
- 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 Revision 3 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 HRS officials responsible for USAS, including IT security controls in place as of January 2013.

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

The criteria used in conducting this audit include:

- OPM Information Technology 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 3, Recommended Security Controls for Federal Information Systems and Organizations;
- 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 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 and remotely with HRTT. This was our first audit of the security controls surrounding USAS.

Compliance with Laws and Regulations

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

Results

I. Security Assessment and Authorization

A Security Assessment and Authorization (SA&A) of USAS was completed in July 2011.

OPM's Chief Information Security Officer reviewed the USAS 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 25, 2011.

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

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 USAS FIPS 199 Security Categorization Template analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. USAS 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 USAS appears to be consistent with FIPS 199 and NIST SP 800-60 requirements, and we agree with the categorization of moderate.

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 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 USAS was created using the template outlined in NIST SP 800-18. 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.

The USAS SSP adequately addresses each of the elements required by NIST. However, we did discover that one security control was inappropriately labeled as a common/inherited control when test results indicate that it is a hybrid control. We brought this to the attention of USAS officials who agreed to review the entire SSP and appropriately modify the control classifications if necessary. While it is important to appropriately classify security controls in the SSP, we do not believe that this typographical error should result in a formal audit finding.

IV. Security Assessment Plan and Report

A Security Assessment Plan (SAP) and Security Assessment Report (SAR) were completed for USAS in June and July 2011 as a part of the system's SA&A process. The SAP and SAR were conducted by a contractor, Capricorn Systems, which was operating independently from HRTT. 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 3, Recommended Security Controls for Federal Information Systems and Organizations.

The SAP outlined the assessment approach, scanning authorization, and test methods. The SAR identified 15 control weaknesses that were discovered as a result of vulnerability scans; 14 of those weaknesses have been remediated, and the remaining weakness was added to the USAS Plan of Action & Milestones (POA&M). A risk rating was applied to each weakness to determine the potential impact of exploitation.

We also reviewed the Security Assessment results table that contained the detailed results of the NIST SP 800-53 Revision 3 controls testing. The table indicated that two controls were not fully satisfied. However, as explained in section VIII below, the controls in question were in place during the security assessment.

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

V. 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 assessment is not being conducted on a system, the system's owner must conduct an internal self-assessment of security controls.

HRTT conducted a self-assessment of the system in August 2012. The assessment included a review of the relevant management, operational, and technical security controls outlined in NIST SP 800-53 Revision 3. Nothing came to our attention to indicate that the security controls of USAS have not been adequately tested by HRTT.

VI. 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 USAS contingency plan documents the functions, operations, and resources necessary to restore and resume USAS operations when unexpected events or disasters occur. The USAS contingency plan closely 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 functional test of the USAS contingency plan was conducted by HRTT officials in April 2012. The test involved recovering the USAS database at the off-site recovery location. The testing documentation contained an analysis and review of the results. We reviewed the testing documentation and determined the test conformed to NIST 800-34 Revision 1 guidelines.

VII. 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.

HRS completed an initial privacy screening or Privacy Threshold Analysis (PTA) of USAS and determined that a PIA was required for this system. A PIA was conducted in July 2011 and approved by the system owner and CIO. Nothing came to our attention to indicate that the PTA and PIA were not conducted in accordance with OPM guidelines.

VIII. 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.

We evaluated the USAS 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. We determined that the weakness discovered during the SA&A vulnerability scan was included in the POA&M. However, the two controls identified in the Security Assessment results table as not fully satisfied do not appear on the USAS POA&M. The two controls are NIST SP 800-53 Revision 3 control SI-7, Software and Information Integrity, and AC-4, Information Flow Enforcement.

We presented this information to USAS officials and they informed us that neither control should be on the USAS POA&M. USAS officials indicated that control SI-7 is classified as a hybrid control; the system specific portion of the control is in place and the OCIO portion has not been implemented. USAS officials believe that there was an error in reporting control AC-4. They believe the error was due to accidental oversight in the Security Assessment Report by the assessment team. USAS officials stated that they were not provided any documentation to indicate that the control did not meet compliance at the time of the security assessment.

We were subsequently provided evidence that control AC-4 is in place and that USAS enforces approved authorizations for controlling the flow of information within the system and between interconnected systems. As a result, nothing came to our attention to indicate that there are any current weaknesses in the management of POA&Ms.

IX. NIST SP 800-53 Revision 3 Evaluation

NIST SP 800-53 Revision 3, "Recommended Security 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 USAS. We tested approximately 40 security controls outlined in NIST SP 800-53 Revision 3 that were identified as being system specific or a hybrid control. Approximately 90 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
- Media Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communication Protection

- Identification and Authorization
- System and Information Integrity

These controls were evaluated by interviewing individuals with USAS 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 3 requirements.

Major Contributors to this Report

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

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

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

March 15, 2013

Human Resources
Solutions

MEMORANDUM FOR [redacted] Chief,

FROM: [redacted]
Associate Director, Human Resources Solutions
USA Staffing Authorizing Official
Information Systems Audits Group

SUBJECT: Response to Draft Report "Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's USA Staffing System (Report No. 4A-HR-00-13-024)"

The OPM USA Staffing Program Office and Human Resources Tools and Technology (HRTT) acknowledge and appreciate the work of the Office of Inspector General to evaluate the USA Staffing System's compliance with the Federal Information Security Management Act (FISMA). This memo serves as an official response to the draft report.

No audit recommendations were included in the draft report for reply however, in response to the finding that agencies are not adhering to the licensing agreements, USA Staffing will be contacting the agencies that have license agreements and will reinforce security requirements.

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

cc:

[redacted]
Senior Team Leader
Office of Audits
Office of the Inspector General

[redacted]
Director
Internal Oversight and Compliance

[redacted]
Director Federal Staffing
Group

[redacted]
Manager
Human Resources Tools & Technology

[redacted]
Designated Security Officer
Human Resources Tools & Technology

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