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 STAFFING SYSTEM

Report Number 4A-HR-00-18-013
May 10, 2018

EXECUTIVE SUMMARY

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

Report No. 4A-HR-00-18-013 **May 10, 2018**

Why Did We Conduct the Audit?

The USA Staffing System is one of the U.S. Office of Personnel Management's (OPM) major information technology (IT) systems. The Federal Information Security Modernization Act (FISMA) requires that the Office of the Inspector General (OIG) perform an audit of IT security controls of this system.

What Did We Audit?

The OIG completed a performance audit of the USA Staffing System to ensure that the system's security controls meet the standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual, 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 USA Staffing System determined that:

- The USA Staffing System Security Assessment and Authorization (Authorization) was updated in September 2017, and an Authorization to Operate was granted for up to three years.
- The security categorization of the USA Staffing System is consistent with Federal Information Processing Standards 199 and NIST Special Publication (SP) 800-60, and we agree with the categorization of "moderate."
- OPM completed a Privacy Impact Assessment for the USA Staffing System.
- The System Security Plan for the USA Staffing System follows the OCIO template, but the system inventory includes instances of unsupported software.
- An independent assessor conducted security controls testing and assessed identified risks for the USA Staffing System.
- The USA Staffing System has been subject to routine testing as part of OPM's continuous monitoring program.
- OPM developed and tested a contingency plan for the USA Staffing System that is generally in compliance with NIST SP 800-34, Revision 1, and the OCIO guidance.
- The USA Staffing System Plan of Action and Milestones documentation from the most recent Authorization does not include all identified weaknesses.
- We evaluated a subset of the system controls outlined in NIST SP 800-53, Revision 4. We determined most of the security controls tested appear to be in compliance, however we did note two areas for improvement.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
HRS	**Human Resources Solutions**
IT	**Information Technology**
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**
POA&M	**Plan of Action and Milestones**
SP	**Special Publication**

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. It requires (1) annual agency program reviews, (2) annual Inspector General evaluations, (3) agency reporting to the U.S. Office of Management and Budget (OMB) the results of Inspector General evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In 2014, Public Law 113-283, the Federal Information Security Modernization Act (FISMA) was established and reaffirmed the objectives of the prior Act. This was our first audit of the USA Staffing System.

The USA Staffing System is a web-based application used by human resources personnel to create and manage position vacancy announcements, application assessments and job questionnaires. Job applicants use the system to apply for open jobs, and hiring managers use it to select their candidates. The USA Staffing System is in the process of being upgraded, and there are currently two active versions, legacy and upgrade. Both versions are included in the scope of this audit.

The U.S. Office of Personnel Management (OPM)'s Office of the Chief Information Officer (OCIO) and OPM's Human Resources Solutions (HRS), share responsibility for implementing and managing the information technology (IT) security controls of the USA Staffing System. We discussed the results of our audit with the OCIO and HRS representatives at an exit conference.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Our objective was to perform an audit of the security controls for the USA Staffing System to ensure that OCIO and HRS 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, and OPM's OCIO.

We accomplished our audit objective by reviewing the degree to which a variety of security program elements were implemented for the USA Staffing System, including:

- Security Assessment and Authorization (Authorization);
- Federal Information Processing Standards (FIPS) 199 Analysis;
- Privacy Impact Assessment;
- System Security Plan;
- Security Assessment Plan and Report;
- Continuous Monitoring;
- Contingency Planning and Contingency Plan Testing;
- Plan of Action and Milestones Process (POA&M); and
- NIST Special Publication (SP) 800-53, Revision 4, Security Controls.

SCOPE AND METHODOLOGY

We conducted this performance audit in accordance with the Generally Accepted 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 security controls and

FISMA compliance efforts of OPM officials responsible for the USA Staffing System, including the evaluation of IT security controls in place as of January 2018.

We considered the USA Staffing 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 representatives of OPM's OCIO and HRS with security responsibilities for the USA Staffing System, 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 USA Staffing 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 USA Staffing System 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 I, Responsibilities for Protecting and Managing Federal Information Resources;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- The Federal Information System Controls Audit Manual;
- NIST SP 800-12, Revision 1, An Introduction to Information 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 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, we conducted the audit in accordance with the Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States.

The OPM Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended, performed the audit. The OIG conducted the audit from November 2017 through January 2018 at OPM's Washington, D.C. office.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether OPM's management of the USA Staffing System is consistent with applicable standards. While generally compliant, with respect to the items tested, OPM was not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. SECURITY ASSESSMENT AND AUTHORIZATION

The USA Staffing System has a current and valid Authorization.

A Security Assessment and Authorization (Authorization) includes 1) a comprehensive assessment that attests that a system's security controls are meeting the security requirements of that system and 2) an official management decision to authorize operation of an information system and accept its known risks. OMB's Circular A-130, Appendix I, mandates that all Federal information systems have a valid Authorization. Although OMB previously required periodic Authorizations every three years, Federal agencies now have the option of continuously monitoring their systems to fulfill the Authorization requirement. However, OPM does not yet have a mature program in place to continuously monitor system security controls, therefore a current Authorization is required for every OPM system.

In September 2017 OPM granted an Authorization to Operate that includes both the legacy and upgraded versions of the system. This Authorization to Operate is valid for up to three years and includes the requirement that the system owner monitor and remediate identified weaknesses on an ongoing basis.

Nothing came to our attention to indicate that the USA Staffing System Authorization to Operate was inadequate.

B. FIPS 199 ANALYSIS

The E-Government Act of 2002 requires Federal agencies to categorize all Federal information and information systems. FIPS 199 provides guidance on how to assign appropriate categorization levels for information security according to a range of risk levels.

NIST SP 800-60 Volume I, 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 USA Staffing System security categorization documentation analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. The USA Staffing System is assessed as having a "moderate" impact level for each area, resulting in an overall categorization of "moderate."

Nothing came to our attention to indicate that the USA Staffing System security categorization was inadequate.

C. PRIVACY IMPACT ASSESSMENT

The E-Government Act of 2002 requires agencies to perform a Privacy Threshold Analysis of Federal information systems to determine if a Privacy Impact Assessment is required for that system. A Privacy Threshold Analysis was performed on the USA Staffing System in July 2017, and it was determined that a Privacy Impact Assessment was required for this system.

OMB Memorandum M-03-22 outlines the necessary components of a Privacy Impact Assessment. The purpose of the assessment is to evaluate and document any personally identifiable information maintained by an information system. The Privacy Impact Assessment was complete and was formally approved and signed by the Chief Privacy Officer in July 2017.

We did not detect any issues with the Privacy Impact Assessment performed for the USA Staffing System.

D. SYSTEM SECURITY PLAN

Federal agencies must implement, for 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 for each system, and provides guidance for doing so.

The USA Staffing System's System Security Plan was developed using the OCIO's System Security Plan template that utilizes NIST SP 800-18, Revision 1, as guidance. The template requires that the System Security Plan contain the following elements:

- System Name and Identifier;
- System Owner;
- Other Designated Contacts;
- System Operational Status;
- General Description/Purpose;
- System Categorization;
- Authorizing Official;
- Assignment of Security Responsibility;

- Information System Type;
- System Environment;
- Laws, Regulations, and Policies Affecting the System;
- Security Control Selection.
- Completion and Approval Dates;
- Minimum Security Controls;
- System Interconnection/Information Sharing; and

We reviewed the current USA Staffing System's System Security Plan, signed in August 2017, and determined that it does include the necessary information, approvals, and supporting documentation. We did identify one issue with the USA Staffing System's System Security Plan.

1) Unsupported Software Platform

The system's software inventory includes an operating platform that is no longer supported by the vendor. Unsupported software does not receive updates and security patches.

OMB Circular A-130 requires that "Agencies shall: … Prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement;" and details that this "Includes hardware, software, or firmware components no longer supported by developers, vendors, or manufacturers through the availability of software patches, firmware updates, replacement parts, and maintenance contracts."

The system inventory includes software that is no longer supported by the vendor.

Failure to remove unsupported software increases the risk that system weaknesses could be exploited.

Recommendation 1

We recommend that OPM upgrade the unsupported operating platform hosting the USA Staffing System.

OPM Response:

"We concur. The [redacted] software in question is currently in use by the Legacy version of [the USA Staffing System]. The Legacy servers are scheduled for a phased decommission starting [redacted] but we have started upgrades where possible while not impacting mission critical functions. The outdated [redacted] software does not impact [the USA Staffing System's] Upgrade version."

OIG Comment:

As part of the audit resolution process, we recommend that the OCIO provide OPM's Internal Oversight and Compliance office with evidence that this recommendation has been implemented. This statement applies to all subsequent recommendations in this audit report that HRS agrees to implement.

E. SECURITY ASSESSMENT PLAN AND REPORT

The USA Staffing System's Security Assessment Plan and Security Assessment Report were completed by OPM in August and September of 2017, respectively, as a part of the system's Authorization process. We reviewed the relevant 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.

Nothing came to our attention to indicate that the USA Staffing System's Security Assessment Plan and Report were inadequate.

F. CONTINUOUS MONITORING

The USA Staffing System security controls were subject to routine testing as a part of continuous monitoring.

OPM requires that the IT security controls of each application be assessed on a continuous basis. OPM's OCIO has developed an Information Security Continuous Monitoring Plan that includes a template outlining the security controls that must be tested for all information systems. All system owners are required to tailor the Information Security Continuous Monitoring Plan template to each individual system's specific security control needs and then test the system's security controls on an ongoing basis. The test results must be provided to the OCIO on a routine basis for centralized tracking.

We did not detect any issues with the USA Staffing System continuous monitoring submissions thus far in fiscal year 2018.

G. 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.

1) Contingency Plan

The USA Staffing System contingency plan documents the functions, operations, and resources necessary to restore and resume the USA Staffing System when unexpected events or disasters occur. The contingency plan follows the format suggested by NIST SP 800-34, Revision 1, and OPM's template for contingency plans.

We did not detect any issues with the USA Staffing System contingency plan.

2) Contingency Plan Testing

Contingency plan testing is a critical element of a viable disaster recovery capability. OPM requires that contingency plans for all systems be tested annually to evaluate the plan's effectiveness and the organization's readiness to execute the plan. NIST SP 800-34, Revision 1, provides guidance for testing contingency plans and documenting the results.

The most recent contingency plan test for the USA Staffing System was conducted in April 2017. The functional test was considered successful although the recovery took slightly longer than anticipated.

Nothing came to our attention to indicate that the USA Staffing System contingency plan testing process was inadequate.

H. PLAN OF ACTION AND MILESTONES

A POA&M is a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for known 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.

1) POA&M Review

Three POA&Ms were not included in the most recent Authorization.

The Security Assessment Report, completed as part of the USA Staffing System Authorization, identified 17 control weaknesses, and these were consolidated into 6 POA&M items that were appropriately included in the Authorization package. However, 3 additional POA&M items existed for the USA Staffing System prior to its most recent Authorization, and these 3 items were *not* included in the Authorization package for consideration.

OPM's policy states that "For systems going through a reauthorization, the POA&M also includes all other open and draft weaknesses that are on the existing POA&M as well."

Failure to properly include all POA&Ms in the Authorization package results in the authorizing official granting an Authorization to Operate without having access to all relevant risk information about the system.

Recommendation 2

We recommend that OPM update the USA Staffing System Authorization package to include the missing POA&Ms and re-issue the Authorization to Operate.

OPM Response:

"We concur. The three existing POA&Ms, from prior to the FY2017 Authorization & Assessment, will be added to the [USA Staffing System] FY17 Authorization package and resubmitted to the [USA Staffing System] Authorizing Official for review and appropriate action."

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 USA Staffing System. We tested approximately 40 controls as outlined in NIST SP 800-53, Revision 4, including one or more controls from each of the following control families:

- Access Control;
- Audit and Accountability;
- Configuration Management;
- Contingency Planning;
- Identity and Authentication;
- Planning;
- Risk Assessment;
- Security Assessment and Authorization;
- System and Communications Protection; and
- System and Information Integrity.

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

We determined that the tested security controls appear to be in compliance with NIST SP 800-53, Revision 4, requirements, with the exceptions detailed below.

Configuration deviations for the USA Staffing System have not been documented and approved.

1) Control CM-6 – Configuration Settings

The USA Staffing System security documentation states that the approved server configuration settings for the system follow the Defense Information Systems Agency's Security Technical Implementation Guide. Configuration settings are the system options that are adjusted to enforce or enhance protection of system components and data. We conducted configuration compliance scans on the servers supporting the USA Staffing System to verify that the established settings had been properly applied. However, our scans found over 200 configuration settings that were not in compliance with the Defense Information Systems Agency's Security Technical Implementation Guide. These deviations have not been documented and approved.

NIST SP 800-53, Revision 4, states that "Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers ... ." NIST requires that configuration settings be established and documented and any deviations be documented and approved.

Failure to apply established configuration settings increases the risk that hackers could exploit system weaknesses.

Recommendation 3

We recommend that OPM apply the approved security configuration settings for the USA Staffing System.

OPM Response:

"We concur. All impacted [redacted] and [redacted] servers along with [the USA Staffing System] Legacy [redacted] servers are scheduled for a phased decommission starting [redacted]. The remaining [USA Staffing System] Upgrade [redacted] servers are scheduled for replacement with [Defense Information Systems Agency's Security Technical Implementation Guide] hardened [redacted]. A phased rollout of [redacted] servers is scheduled to start in [redacted]."

2) Control SI-2 – Flaw Remediation

We also conducted credentialed vulnerability scans on the servers supporting the USA Staffing System looking for security weaknesses. The results of our scans indicate several servers were missing critical patches that had been released more than 30 days before the scans took place. The specific vulnerabilities found by the scans were provided to OPM personnel, but will not be detailed in this report.

Several of the USA Staffing System servers were missing patches more than 30 days old.

NIST SP 800-53, Revision 4, requires that, "The organization: ... Identifies, reports, and corrects information systems flaws ... [and] Installs security-relevant software and firmware updates ... ."

Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses.

Recommendation 4

We recommend that OPM apply system patches in a timely manner and in accordance with policy.

OPM Response:

"We concur. We have mitigated 75% of the server scan related and web-based findings identified within the OIG Audit Inquiry 01. The remaining 25% of identified findings will be addressed in conjunction with the phased Legacy server and web-based interface decommissioning starting [redacted], the phased rollout of [redacted] servers scheduled to start in [redacted], and the Upgrade software release [redacted] scheduled for [redacted]."

APPENDIX

March 20, 2018

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

FROM: ROBERT M. LEAHY
Deputy Chief Information Officer

DIANNA SAXMAN
Deputy Associate Director, Federal Staffing Center
Human Resources Solutions

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

Report No. 4A-MO-00-18-013

Thank you for providing OPM the opportunity to respond to the Office of the Inspector General (OIG) draft report, Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's USA Staffing System, 4A-MO-00-18-013.

Responses to your recommendations including planned corrective actions, as appropriate, are provided below.

Recommendation 1: We recommend that OPM upgrade the unsupported operating system hosting the USAS.

Management Response: We concur. The [redacted] software in question is currently in use by the Legacy version of USAS. The Legacy servers are scheduled for a phased decommission starting [redacted] but we have started upgrades where possible while not impacting mission critical functions. The outdated [redacted] software does not impact USAS's Upgrade version.

Recommendation 2: We recommend that OPM update the USAS Authorization package to include the missing POA&Ms and re-issue the ATO.

Management Response: We concur. The three existing POA&Ms, from prior to the FY2017 Authorization & Assessment, will be added to the USAS FY17 Authorization package and resubmitted to the USAS Authorizing Official for review and appropriate action.

Recommendation 3: We recommend that OPM apply the approved security configuration settings for the USAS.

Management Response: We concur. All impacted [redacted] and [redacted] servers along with USAS Legacy [redacted] servers are scheduled for a phased decommission starting [redacted]. The remaining USAS Upgrade [redacted] servers are scheduled for replacement with DISA STIG hardened [redacted] servers. A phased rollout of [redacted] servers is scheduled to start in [redacted].

Recommendation 4: We recommend that OPM apply system patches in a timely manner and in accordance with policy.

Management Response: We concur. We have mitigated 75% of the server scan related and web-based findings identified within the OIG Audit Inquiry 01. The remaining 25% of identified findings will be addressed in conjunction with the phased Legacy server and web-based interface decommissioning starting [redacted], the phased rollout of [redacted] servers scheduled to start in [redacted], and the Upgrade software release [redacted] scheduled for [redacted].

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact [redacted], [redacted], and [redacted]@opm.gov.

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