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 ENTERPRISE HUMAN RESOURCES INTEGRATION DATA WAREHOUSE

Report Number 4A-CI-00-19-006
June 17, 2019

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Enterprise Human Resource Integration Data Warehouse

Report No. 4A-CI-00-19-006 **June 17, 2019**

Why Did We Conduct The Audit?

The Enterprise Human Resource Integration Data Warehouse (EHRIDW) is one of the U.S. Office of Personnel Management's major information technology (IT) systems. The Federal Information Security Modernization Act requires that the Office of the Inspector General perform audits of IT security controls of agency systems.

What Did We Audit?

The Office of the Inspector General completed a performance audit of the EHRIDW to ensure that the system's security controls meet the standards established by the Federal Information Security Modernization Act, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual, and the U.S. Office of Personnel Management's Office of the Chief Information Officer.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls of the EHRIDW determined that:

- Six of the seven required EHRIDW Security Assessment and Authorization (Authorization) security documents we reviewed were out of date and/or inaccurate at the time the Authorization was granted.
- The EHRIDW security categorization is consistent with both the Federal Information Processing Standards 199 and NIST Special Publication (SP) 800-60, and we agree with the "high" categorization. However, the document was not signed by the current System Owner, Chief Information Security Officer, or Authorizing Official.
- The EHRIDW Privacy Threshold Analysis and Privacy Impact Assessment are out of date and contain information inconsistent with other system documentation.
- The EHRIDW System Security Plan follows the Office of the Chief Information Officer's template, but does not adequately reflect the state of the system at the time of fieldwork.
- An independent security assessment was not conducted on EHRIDW prior to the Authorization being granted.
- Continuous Monitoring for EHRIDW was conducted in accordance with the agency's quarterly schedule for FY 2018.
- The EHRIDW contingency plan is out of date, inaccurate, and has not been tested annually.
- The EHRIDW Plan of Action and Milestones documentation is not up to date and contains 65 identified weaknesses that are at least a year old and past their scheduled completion dates.
- 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 several areas for improvement regarding policy and procedures, role-based security training and vulnerability scanning.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
EHRIDW	**Enterprise Human Resource Integration Data Warehouse**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
OCIO	**Office of the Chief Information Officer**
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**
SSP	**System Security Plan**

TABLE OF CONTENTS

APPENDIX: OPM's May 3, 2019, response to the draft audit report, issued March 27, 2019.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

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.

The Enterprise Human Resource Integration Data Warehouse (EHRIDW) is one of the agency's major information technology systems. The U.S. Office of Personnel Management (OPM) uses the EHRIDW to collect, integrate, and publish data for 2.2 million Executive Branch employees on a bi-weekly basis, supporting agency and government-wide analytics. This was our first audit of the EHRIDW information technology controls.

OPM's Office of the Chief Information Officer (OCIO) and the Data Warehouse Program office share responsibility for implementing and managing the information technology (IT) security controls of the EHRIDW. We discussed the results of our audit with the OCIO and Data Warehouse Program representatives at an exit conference.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Our objective was to perform an evaluation of the security controls for the EHRIDW to ensure that the OCIO and Data Warehouse Program officials 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.

The audit objective was accomplished by reviewing the degree to which a variety of security program elements were implemented for the EHRIDW, including:

- Security Assessment and Authorization (Authorization);
- Federal Information Processing Standards Publication 199 (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 EHRIDW, including the evaluation of IT security controls in place as of January 2019.

We considered the EHRIDW 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 objective.

To accomplish our objective, we interviewed representatives of OPM's OCIO and the Data Warehouse Program with security responsibilities for the EHRIDW, 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 EHRIDW 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 EHRIDW internal controls taken as a whole. The criteria used in conducting this audit include:

- OPM Information Security Privacy and Policy Handbook;
- OPM Security Assessment and Authorization Guide;
- OMB Circular A-130, Appendix I, Responsibilities for Protecting and Managing Federal Information Resources;
- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002;
- 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 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems;

- NIST SP 800-34, Revision 1, Contingency Planning Guide for 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, Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories; and

- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

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 performed the audit, as established by the Inspector General Act of 1978, as amended. We conducted the audit from October 2018 through January 2019 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 EHRIDW 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

Security documents required for an Authorization were out of date and inaccurate at the time the Authorization was granted.

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 an Authorization is required for all OPM systems at least once every three years as required by OPM policy.

EHRIDW underwent a data center migration from Lakewood, Colorado to Macon, Georgia in the summer of 2017. In December 2017, the system was granted an Authorization for 120 days. Previously, the EHRIDW system was managed by a contractor until April 2018 when the contract was not renewed. Management of the EHRIDW system was transferred to OPM employees in Macon. In April 2018, OPM granted a one year Authorization to Operate to the EHRIDW until April 2019. Fieldwork for this audit concluded in January 2018. As of the date of OPM's response to the draft report, a new Authorization package had not been finalized and approved. As such, this report details our review of the documentation supporting the 2018 Authorization.

As we will demonstrate throughout this report, we observed that six of the seven security documents required for an Authorization were out of date and inaccurate at the time the Authorization was granted.

According to the OPM Security Assessment and Authorization Guide, "Security documentation is most effective when it's continually updated as the security of a system is changed. This continual update of security documentation makes the authorization process more efficient. At a minimum the [System Security Plan], [Contingency Plan], [Privacy Threshold Analysis] (and [Privacy Impact Assessment] if required) must be updated annually."

Given that EHRIDW had undergone significant changes prior to the Authorization, documentation accurately reflecting the current state of the system becomes even more crucial when granting an Authorization to identify any new risks of the system to the organization the changes may have created.

Recommendation 1

We recommend that OPM ensure all Authorization documents are updated to be accurate, current, and approved by the appropriate officials for the 2019 Authorization.

OPM Response:

"We concur with the recommendation. OPM understands the importance of maintaining up-to-date Authorization documentation. OPM has updated EHRIDW Authorization documents to be accurate, current, and approved by the appropriate official. OPM will coordinate the submission of security authorization documents with its Internal Oversight and Compliance office after the assessment of the system is completed."

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 also applies to all subsequent recommendations in this audit report that OCIO agrees to implement.

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, Revision 1, 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 199.

The EHRIDW security categorization documentation analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. The EHRIDW has a "high" confidentiality and integrity impact and a "moderate" availability impact, resulting in an overall system categorization of "high."

While the system security categorization was accurate, it appears that the FIPS 199 was rolled forward from a prior Authorization package without the required review and approval. We

observed that the document was signed in May 2017 by a different System Owner, Chief Information Security Officer and Authorizing Official than the individuals in those roles at the time of the most recent Authorization.

According to the OPM Security Assessment and Authorization Guide, "For existing systems undergoing re-authorization, this step involves a review of existing system categorization for currency."

A system's FIPS 199 documentation that is not reviewed and signed by the current System Owner, Chief Information Security Officer and Authorizing Official can indicate a lack of understanding of the system's categorization, for which they are responsible.

Recommendation 2

We recommend that OPM ensures the EHRIDW Security Categorization (FIPS 199) is reviewed and signed by the current System Owner, Chief Information Security Officer and Authorizing Official at the time of the Authorization to Operate.

OPM Response:

"We concur with the recommendation. OPM has completed a thorough review and approval of updates to the EHRIDW Security Categorization (FIPS 199). OPM will coordinate the submission of security authorization documents with its Internal Oversight and Compliance office after the assessment of the system is completed."

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 EHRIDW in March 2015. As such, the Privacy Threshold Analysis is out of date and does not contain information consistent with the more recent System Security Plan and FIPS 199 documentation and lists a prior System Owner. In addition the document was incomplete as it was not reviewed by the OPM Privacy Office and the designation requiring a Privacy Impact Assessment was not selected.

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. Despite an incomplete Privacy Threshold Analysis, a Privacy Impact Assessment was last updated in January 2016. As with the Privacy Threshold Analysis, the system information listed in the Privacy Impact Analysis is not consistent with the information in the most recent System Security Plan. In addition, the document had not been reviewed and approved by the System Owner and Chief Information Security Officer at the time of the Authorization.

According to the OPM Security Assessment and Authorization Guide, "At a minimum the [System Security Plan], [Contingency Plan], [Privacy Threshold Analysis] (and [Privacy Impact Assessment] if required) must be updated annually."

Out of date and incomplete Privacy Threshold Analysis and Privacy Impact Analysis documents can mislead the current System Owner, Chief Information Security Officer, and Authorizing Official on the overall privacy impact of the system.

Recommendation 3

We recommend that OPM update the EHRIDW Privacy Threshold Analysis and Privacy Impact Analysis documents according to OPM policy.

OPM Response:

"We concur with the recommendation. OPM understands the importance of keeping the privacy documentation updated. OPM has implemented updated the Privacy Threshold Analysis. The Privacy Impact Assessment … is in process of being updated. OPM will coordinate the submission of these privacy documents with its Internal Oversight and Compliance office once the updated [Privacy Impact Assessment] is approved."

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 (SSP) for each system, and provides guidance for doing so.

The Data Warehouse Program office developed the EHRIDW SSP using the OCIO's SSP template that utilizes NIST SP 800-18, Revision 1, as guidance. The template requires the SSP to contain the following elements:

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

The current EHRIDW SSP was last updated in July 2017 and does not adequately reflect the system's current state. The document includes the Lakewood, Colorado data center in the system's information flow and describes the intent to migrate the system to Macon, Georgia. At the time of the reauthorization in April 2018, the system was already fully migrated to Macon, Georgia. Our review also identified that the out of date SSP does not accurately reference all of the software currently used by the system and that some points of contact are inaccurately listed. The SSP does not display review and approval by the System Owner and Authorizing Official at the time of the most recent Authorization.

NIST SP 800-18, Revision 1, states that "it is important to periodically assess the plan, review any change in system status, functionality, design, etc., and ensure that the plan continues to reflect the correct information about the system."

An SSP that is outdated and inaccurate increases the risks that controls are not implemented and functioning as required. This also increases the difficulty of assessing and addressing risks to the system and to OPM as a whole.

Recommendation 4

We recommend that OPM update the EHRIDW SSP to reflect the current state of the system and ensure it meets OPM policies and NIST guidelines.

OPM Response:

"We concur with the recommendation. OPM has updated the System Security Plan … to reflect the current location of the system. It is aligned to OPM policies and NIST guidelines. OPM will coordinate the submission of security authorization documents with its Internal Oversight and Compliance office after the assessment of the system is completed."

E. SECURITY ASSESSMENT PLAN AND REPORT

A Security Assessment Plan describes the scope, procedures, environment, team, roles, and responsibilities for an assessment to determine the effectiveness of a system's security controls.

The EHRIDW Security Assessment Plan is a draft version created by the OCIO Information Security Officer in December 2017. The EHRIDW Security Assessment Report is an addendum, also created by the OCIO Information Security Officer in April 2018. An independent assessment was not conducted for the Authorization granted in April 2018.

An independent assessment was not conducted for the Authorization granted in April 2018.

According to the OPM Security Assessment and Authorization Guide, "Moderate and High impact systems require assessment by an independent assessor for authorization."

Failure to conduct an independent assessment of security controls may increase the likelihood of exploitation of unknown vulnerabilities.

Recommendation 5

We recommend that OPM conduct a full independent assessment of security controls for the EHRIDW 2019 Authorization.

OPM Response:

"We concur with the recommendation. OPM is currently undertaking a full independent security assessment of OPM EHRIDW system. OPM will coordinate the submission of security authorization documents with its Internal Oversight and Compliance office after the assessment of the system is completed."

F. CONTINUOUS MONITORING

OPM requires that the IT security controls of each system 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 received the FY 2018 quarterly continuous monitoring submissions for EHRIDW. A review of the submissions revealed that over 160 distinct controls were tested.

Nothing came to our attention to indicate that the EHRIDW continuous monitoring process was inadequate.

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 EHRIDW contingency plan was created in March 2017 and is out of date, containing inaccurate pre-migration information. The document refers to Lakewood, Colorado as the current location for the system. The roles and responsibility section includes individuals no longer associated with the system. The contingency plan is not signed by the current System

Owner. Additionally, a contingency plan test was conducted in April 2017 and the plan was not updated to reflect the test results. As with the other required security documentation, the EHRIDW contingency plan was not updated prior to the most recent Authorization.

According to OPM policy, "The system owner (SO) shall ensure the contingency plan is reviewed for the information system at least annually and is revised to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing."

An outdated and inaccurate contingency plan can cause additional confusion and exacerbate outages during an incident.

Recommendation 6

We recommend that OPM update the EHRIDW contingency plan in accordance with the OPM template and policies.

OPM Response:

"We concur with the recommendation. In 2019, the OPM EHRIDW Contingency Plan has been reviewed, updated, and approved by the appropriate OPM official in accordance with OPM policy. OPM will coordinate the submission of security authorization documents with its Internal Oversight and Compliance office after the assessment of the system is completed."

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 EHRIDW contingency plan test was conducted in April 2017, before the system migrated to OPM's Macon, Georgia data center. After the migration occurred and prior to the April 2018 Authorization, EHRIDW did not conduct a contingency plan test.

According to OPM policy, "The contingency plan for the information system is tested and/or exercised at least annually using OPM defined and information system specific tests and exercises such as checklist, walk-through/tabletop, simulation, parallel, full interrupt to determine the plan's effectiveness and the organization's readiness to execute the plan … ."

If a contingency plan test is not conducted annually, the effectiveness of the plan cannot be determined and all system personnel may not know their roles in the event of a disaster.

Recommendation 7

We recommend that OPM conduct a test of an updated EHRIDW contingency plan in accordance with the OPM policies.

This recommendation cannot be addressed until Recommendation 6 has been completed.

OPM Response:

"We concur with the recommendation. OPM will test the updated EHRIDW contingency plan in accordance with OPM policies."

H. PLAN OF ACTION AND MILESTONES

All of the 65 documented EHRIDW weaknesses were identified over a year ago, including 23 that were identified by November 2016.

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.

The EHRIDW POA&M is properly formatted and all of the weaknesses in the POA&M are properly documented according to OPM policy. However, the POA&M has 65 open weaknesses identified and all of them are past their scheduled completion dates. All of the 65 weaknesses were identified over a year ago, including 23 that were identified by November 2016. Additionally, while seven identified weaknesses are pending closure, they have been pending for over a year.

The current EHRIDW Authorization to Operate letter requires continued mitigation and/or remediation of open POA&M items identified as a result of required continuous monitoring

activities within the following timeframes of the date of this document: Critical/High risk: 30 days, Medium risk: 60 days, Low risk: 120 days.

OPM's guidance states that "Should expected completion dates for milestones of POA&Ms be missed, the associated POA&Ms will be brought before the [Management Review Board] for review in order to address any corrective actions needed for remediating the POA&Ms in accordance with the requirements defined in the Authorization to Operate … issued for the applicable system. Updated milestones and expected completion dates will be required for the following Management Review Board meeting."

Failure to update the POA&M increases the likelihood of weaknesses not being addressed in a timely manner and potentially exposing the system to malicious attacks exploiting those unresolved vulnerabilities.

Recommendation 8

We recommend that OPM revise and/or develop detailed action plans to remediate all overdue EHRIDW POA&M items. These revised action plans should include new estimated completion dates supported by the milestones documented in the revised action plans. Additionally, these plans should be presented to the Management Review Board.

OPM Response:

"We concur with the recommendation. OPM has updated the Plan of Action and Milestones … for the EHRIDW system. OPM will coordinate the submission of security authorization documents with its Internal Oversight and Compliance office after the assessment of the system is completed."

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 OPM has implemented a subset of these controls for the EHRIDW. 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;
- Awareness and Training;
- Configuration Management;
- Contingency Planning;
- Identity and Authentication;
- Incident Response;
- Planning;
- Risk Assessment;
- Security Assessment and Authorization;
- System and Information Integrity; and
- System and Services Acquisition.

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

1. Control AT-3 – Role-Based Security Training

NIST requires role-based security training for systems with a categorization level of "high." Role-based training should be provided to any individual with access to system-level software which can include, but is not limited to "enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, [and] security control assessors." Training would include "adequate security-related technical training specifically tailored for their assigned duties."

OPM requires all agency employees to complete annual security/privacy awareness training, however, this differs from role-based security training. Currently OPM does not provide role-based security training for EHRIDW personnel.

NIST SP 800-53, Revision 4, requires that an organization "Provides role-based security training to personnel with assigned security roles and responsibilities: … Before authorizing

access to the information system or performing assigned duties; … When required by information system changes; and … thereafter."

Failure to provide role-based security training for the EHRIDW personnel with system level access, especially after significant changes to the system, increases the likelihood of user error, possibly exposing the system to additional risks.

Recommendation 9

We recommend that OPM provide and document role-based security training for the EHRIDW personnel with system level access.

OPM Response:

"We concur with the recommendation. OPM requires individuals (database and system administrators, etc.) that have security roles and responsibilities which require privilege access to perform security operational functions and mechanisms to complete security role-based training. OPM will evaluate where EHRIDW personnel hold significant security responsibilities and add those individuals to its enterprise list for the next training period."

2. Control AU-1 – Audit Policies and Procedures

Audit and accountability policies and procedures can help in detecting security violations, performance problems, and application flaws. OPM has an agency-wide policy for Auditing and Accountability and procedures in place to enable the implementation of the policy for EHRIDW. However, OPM personnel involved in the auditing process were not aware of the procedures.

NIST SP 800-53, Revision 4, requires that an organization "Develops, documents, and disseminates … Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls … ."

Auditing procedures that are not disseminated can lead to ineffective auditing, increasing the likelihood that security violations are undetected.

Recommendation 10

We recommend that OPM disseminate auditing procedures to the individuals with auditing responsibilities and ensure the current process complies with the documented procedures.

OPM Response:

"We concur with the recommendation. OPM has identified the procedures described by the OIG and is providing the Information Technology Security FISMA Procedures along with this response."

OIG Comment:

We have reviewed the auditing procedures provided by OPM and have found them to be sufficient. The recommendation was revised accordingly.

3. Control CA-8 – Penetration Testing Results Remediation

We requested evidence of penetration testing of the EHRIDW system. OPM provided a penetration test report for another system that included servers and databases from EHRIDW. After reviewing the report, we observed some vulnerabilities were detected that impacted the EHRIDW system. However, POA&Ms were not created for all of the identified vulnerabilities. OPM's current procedures do not specifically address the remediation of penetration testing results.

According to NIST SP 800-53, Revision 4, "Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries." and "The organization … Updates existing plan of action and milestones … based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities."

Penetration test results that are not tracked in POA&Ms raise the risk that the vulnerabilities are not remediated and therefore increases the likelihood of exploitation.

Recommendation 11

We recommend that OPM update the current policies and procedures to include the remediation of penetration testing results.

OPM Response:

"We concur with the recommendation. OPM has identified the policies and procedures described by the OIG and is providing the OPM Risk Management Policy and OPM POA&M Guide along with this response."

OIG Comment:

We acknowledge that the policy and guide provided in OPM's response to the draft do address identifying and recording weaknesses from a variety of sources. However, these do not specifically address penetration testing as a method for identifying and assessing risks to the system. In the case of EHRIDW this policy and guide were not sufficient to ensure the identified risks were captured and tracked for corrective action. OPM should assess the policy and guide to identify improvements to better ensure risks from penetration testing are appropriately captured. Once this assessment occurs, steps should be taken to disseminate the guidance to the relevant stakeholders and ensure there is a clear understanding of the ISSO responsibilities to report and track all known weaknesses, including those resulting from penetration testing.

4. Control SA-1 – Policy and Procedures Providing Guidance for the Transition of a System's Management

As discussed above, contractors managed the EHRIDW system until April 2018. When the contract was not renewed, OPM employees located in OPM's Macon data center assumed management of EHRIDW effective June 2018. The OPM employees responsible for managing the system indicated that the technical and program offices are still learning how to properly manage the system as a result of insufficient knowledge transfer at the time of system transition.

OPM does not have any policies and procedures pertaining to the knowledge transfer required for a successful transition of a system's management between entities (e.g., from contractors to OPM employees, and conversely from OPM employees to contractors).

NIST SP 800-53, Revision 4, requires that the organization, "Develops, documents, and disseminates … A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and … Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls … ."

An ad-hoc process for transitioning the management and control of a system between entities can result in insufficient planning and increased learning curves, subsequently causing insufficient management and implementation of the system's IT security controls.

Recommendation 12

We recommend that OPM develop policy and procedures to document requirements necessary for transitioning a system's management between entities.

OPM Response:

"We concur with this recommendation. OPM has identified the policies and procedures described by the OIG and is providing the OPM Security Program Policy, Security Authorization Guide, and System Registration Form along with this response."

OIG Comment:

We have reviewed the documentation OPM provided and acknowledge that they address the security requirements for documenting any major system change (e.g., a transition). However, OPM has not provided documentation that provides business level guidance for how to successfully transition a system between responsible entities. Documentation of this nature should include, at a minimum, a knowledge transfer plan.

5. Control RA-5 – Scanning Credentials Management

As a part of this audit, we conducted a vulnerability scanning exercise on the EHRIDW system. During our scanning exercise, we observed multiple instances where the OPM scanning team did not have the appropriate credentials for scanning the EHRIDW servers and databases. In one instance, the audit team communicated directly with an IT Operations Manager for EHRIDW to update the scanning credentials.

OPM has implemented vulnerability scanning procedures, however, the procedures do not ensure the credentials are correct prior to scanning. When scans fail due to incorrect credentials, the credentials are then updated. A series of emails was provided to document the current communication process for updating credentials with the OPM scanning team. These emails evidenced the process for remediating credential failures.

OPM also has an account management plan that contains a password change process. However, the document does not require communicating newly updated credentials to the scanning team. Without notifying the scanning team of the password change, the result is an increased number of failed scans.

NIST SP 800-53, Revision 4, requires that "The organization … Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for … Formatting checklists and test procedures … ."

The importance of using correct credentials for scanning exercises cannot be understated. Failed scans due to incorrect credentials can result in blank scan results, which initiate a timely process to validate credentials and rescan systems. While OPM maintains a minimum requirement for monthly scanning, a business decision was made to scan EHRIDW weekly. Incorrect scanning credentials can impede on OPM's ability to achieve vulnerability scanning objectives. More importantly, they may result in vulnerabilities not being detected in a timely manner and increasing both the time until remediation and the likelihood the vulnerabilities could be exploited.

Recommendation 13

We recommend that OPM update current procedures to include requirements for timely communication of updated scanning credentials to the OPM scanning team.

OPM Response:

"We do not concur with this recommendation. OPM has provided evidence to OIG to show that scanning errors are communicated to the appropriate individuals within the OPM scanning team and are resolved in a timely manner. At this time, as we do not agree with the finding, we are not planning to implement corrective actions."

OIG Comment:

We acknowledge that OPM has a process in place to resolve scanning errors once they occur and that this recommendation would not eliminate the need for such a policy. Changed passwords are not the only reason for failed scans and proactively notifying the scanning team would remove this source of failed scans. This would increase the visibility into EHRIDW's potential vulnerabilities, enabling more prompt remediation of weaknesses that could be exploited. The documentation OPM provided shows that in isolated instances remediation of credential errors took up to two weeks to resolve. While this is still within the minimum monthly scanning requirements, it does not achieve the weekly scanning objectives outlined in scanning procedures. Any scanning credential errors that can be eliminated by proactive notifications of password changes would be an improvement both in security and efficiency.

6. Control RA-5 – Scanning Full EHRIDW Inventory

OPM provided the EHRIDW primary server and database vulnerability scan results from August and September 2018. Our review of the scans revealed that not all of the 36 servers and databases in the EHRIDW system inventory underwent vulnerability scans.

Vulnerability scanning was not conducted on all EHRIDW servers and databases in the inventory.

We also requested the scanning results for the 36 disaster recovery servers and databases for August and September 2018. OPM only provided the scanning results for September 2018. Our review of the scan results revealed that three of the remaining five servers, not included in the scan results, are Microsoft Windows production servers. Vulnerability scanning was not conducted on all EHRIDW servers and databases in the inventory.

This finding is consistent with the open recommendation in the FY 18 FISMA audit report (Report No. 4A-CI-00-18-038, Recommendation 28) that requires the OCIO to implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory. As such, no further recommendation is necessary.

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the Chief Information Officer

MAY 0 3 2019

Memorandum For: [redacted]
Chief, Information Systems Audit Group
Office of the Inspector General

From: Clare A. Martorana
Chief Information Officer
U.S. Office of Personnel Management

Subject: Office of Personnel Management Response to the Office of Inspector General Audit of the Information Technology Secuirty Controls of the U.S. Office of Personnel Management's Enterprise Human Resource Integration Data Warehouse (Report No. 4A-CI-00-19-006)

Thank you for providing OPM the opportunity to respond to the Office of the Inspector General (OIG) draft report, Audit of Information Technology Security Controls of the U.S. Office of Personnel Management's Enterprise Human Resources Integration Data Warehouse, 4A-CI-0019-006.

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

Recommendation 1: We recommend that OPM ensure all Authorization documents are updated to be accurate, current, and approved by the appropriate officials for the 2019 Authorization.

Management Response: We concur with the recommendation. OPM understands the importance of maintaining up-to-date Authorization documentation. OPM has updated EHRIDW Authorization documents to be accurate, current, and approved by the appropriate official. OPM will coordinate the submission of security authorization documents with its Internal Oversight and Compliance office after the assessment of the system is completed.

Recommendation 2: We recommend that OPM ensures the EHRIDW Security Categorization (FIPS 199) is reviewed and signed by the current System Owner, Chief Information Security Officer and Authorizing Official at the time of the Authorization to Operate.

Management Response: We concur with the recommendation. OPM has completed a thorough review and approval of updates to the EHRIDW Security Categorization (FIPS 199). OPM will coordinate the submission of security authorization documents with its Internal Oversight and Compliance office after the assessment of the system is completed.

Recommendation 3: We recommend that OPM update the EHRIDW Privacy Threshold Analysis and Privacy Impact Analysis documents according to OPM policy.

Management Response: We concur with the recommendation. OPM understands the importance of keeping the privacy documentation updated. OPM has implemented updated the Privacy Threshold Analysis. The Privacy Impact Assessment (PIA) is in process of being updated. OPM will coordinate the submission of these privacy documents with its Internal Oversight and Compliance office once the updated PIA is approved.

Recommendation 4: We recommend that OPM update the EHRIDW SSP to reflect the current state of the system and ensure it meets OPM policies and NIST guidelines.

Management Response: We concur with the recommendation. OPM has updated the System Security Plan (SSP) to reflect the current location of the system. Itis aligned to OPM policies and NIST guidelines. OPM will coordinate the submission of security authorization documents with its Internal Oversight and Compliance office after the assessment of the system is completed.

Recommendation 5: We recommend that OPM conduct a full independent assessment of security controls for the EHRIDW 2019 Authorization.

Management Response: We concur with the recommendation. OPM is currently undertaking a full independent security assessment of OPM EHRIDW system. OPM will coordinate the submission of security authorization documents with its Internal Oversight and Compliance office after the assessment of the system is completed.

Recommendation 6: We recommend that OPM update the EHRIDW contingency plan in accordance with the OPM template and policies.

Management Response: We concur with the recommendation. In 2019, the OPM EHRIDW Contingency Plan has been reviewed, updated, and approved by the appropriate OPM official in accordance with OPM policy. OPM will coordinate the submission of security authorization documents with its Internal Oversight and Compliance office after the assessment of the system is completed.

Recommendation 7: We recommend that OPM conduct a test of an updated EHRIDW contingency plan in accordance with the OPM policies.

Management Response: We concur with the recommendation. OPM will test the updated EHRI DW contingency plan in accordance with OPM policies.

Recommendation 8: We recommend that OPM revise and/or develop detailed action plans to remediate all overdue EHRIDW POA&M items. These revised action plans should include new estimated completion dates supported by the milestones documented in the revised action plans. Additionally, these plans should be presented to the Management Review Board.

Management Response: We concur with the recommendation. OPM has updated the Plan of Action and Milestones (POA&M) for the EHRIDW system. OPM will coordinate the submission of security authorization documents with its Internal Oversight and Compliance office after the assessment of the system is completed.

Recommendation 9: We recommend that OPM provide and document role-based security training for the EHRIDW personnel with system level access.

Management Response: We concur with the recommendation. OPM requires individuals (database and system administrators, etc.) that have security roles and responsibilities which require privilege access to perform security operational functions and mechanisms to complete security role-based training. OPM will evaluate where EHRIDW personnel hold significant security responsibilities and add those individuals to its enterprise list for the next training period.

Recommendation 10: We recommend that OPM develop auditing procedures to implement the existing Auditing and Accounting Policy.

Management Response: We concur with the recommendation. OPM has identified the procedures described by the OIG and is providing the Inf01mation Technology Security FISMA Procedures along with this response.

Recommendation 11: We recommend that OPM update the current policies and procedures to include the remediation of penetration testing results.

Management Response: We concur with the recommendation. OPM has identified the policies and procedures described by the OIG and is providing the OPM Risk Management Policy and OPM POA&M Guide along with this response.

Recommendation 12: We recommend that OPM develop policy and procedures to develop requirements necessary for transitioning a system's management between entities.

Management Response: We concur with this recommendation. OPM has identified the policies and procedures described by the OIG and is providing the OPM Security Program Policy, Security Authorization Guide, and System Registration Form along with this response.

Recommendation 13: We recommend that OPM update current procedures to include requirements for timely communication of updated scanning credentials to the OPM scanning team.

Management Response: We do not concur with this recommendation. OPM has provided evidence to OIG to show that scanning errors are communicated to the appropriate individuals within the OPM scanning team and are resolved in a timely manner. At this time, as we do not agree with the finding, we are not planning to implement corrective actions.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Cord Chase, 202-606-0117, and Cord.Chase@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