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 ENTERPRISE HUMAN RESOURCES INTEGRATION DATA WAREHOUSE FY 2009

Report No. 4A-HR-00-09-033

Date: June 1, 2009

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S ENTERPRISE HUMAN RESOURCES INTEGRATION DATA WAREHOUSE FY 2009

WASHINGTON, D.C.

Report No. 4A-HR-00-09-033

Date: June 1, 2009

Michael R. Esser
Assistant Inspector General
for Audits

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S ENTERPRISE HUMAN RESOURCES INTEGRATION DATA WAREHOUSE FY 2009

WASHINGTON, D.C.

Report No. 4A-HR-00-09-033

Date: June 1, 2009

This final audit report discusses the results of our review of the information technology security controls of the Enterprise Human Resources Integration Data Warehouse (EHRIDW) System. Our conclusions are detailed in the "Results" section of this report.

The results of our audit are summarized below:

- A self-assessment was not required for EHRIDW in fiscal year (FY) 2008. The Office of the Inspector General (OIG) will verify that a current self-assessment of National Institute of Standards and Technology (NIST) Special Publication 800-53 controls is conducted for this system as part of the FY 2009 general Federal Information Security Management Act audit process.
- A risk assessment was performed for EHRIDW that encompasses the nine primary steps outlined in NIST guidance.
- The EHRIDW information system security plan was prepared in accordance with the format and methodology outlined in NIST guidance.
- An independent system security test and evaluation was conducted for EHRIDW.
- EHRIDW was certified and accredited in FY 2009 in accordance with NIST guidance.

- The EHRIDW contingency plan is routinely maintained and tested in accordance with NIST Guidance.
- An impact analysis based on the Federal Information Processing Standards Publication 199 was completed for EHRIDW in accordance with NIST guidance. The OIG agreed with the "high" classification of the system.
- One of the 13 security controls tested by the OIG was not implemented for EHRIDW.
- The 2009 second quarter Plan of Action and Milestones for EHRIDW appeared to be properly maintained in accordance with Office of Personnel Management policy and guidance from the U.S. Office of Management and Budget.

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 evaluated the information technology (IT) security controls related to the Office of Personnel Management's (OPM) Enterprise Human Resources Integration Data Warehouse (EHRIDW).

Background

EHRIDW is one of OPM's 41 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 Human Resources Line of Business (HRLOB) has been designated with ownership of EHRIDW. EHRIDW is a repository for electronic personnel data of Federal employees and supports several minor applications that are used for analytical purposes by human resources specialists throughout the government.

Although the EHRIDW application is owned and administered by OPM's HRLOB, the infrastructure supporting EHRIDW's production environment is owned and maintained by the Department of the Interior's (DOI) National Business Center (NBC). The production environment is housed at the NBC facility in Ashburn, Virginia, and the development environment is housed at the NBC facility in Denver, Colorado. The technical infrastructure in place at both NBC facilities has been certified and accredited by DOI.

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

Objectives

Our overall objective was to perform an evaluation of security controls for EHRIDW to ensure that HRLOB officials have implemented IT security policies and procedures in accordance with standards established by OPM's Center for Information Services (CIS).

These policies and procedures are designed to assist program office officials in developing and documenting IT security practices that are in substantial compliance with FISMA, as well as OMB regulations and the National Institute of Standards and Technology (NIST) guidance.

OPM's IT security policies and procedures require managers of all major and sensitive 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 overall audit objective was accomplished by

reviewing the degree to which a variety of these security program steps have been implemented for EHRIDW, including:

- Annual Self Assessments;
- Risk and Vulnerability Assessments;
- Information System Security Plans;
- Independent Security Test and Evaluation;
- Certification and Accreditation;
- Contingency Planning;
- Federal Information Processing Standards Publication 199 (FIPS 199) Analysis;
- Evaluation of NIST Special Publication (SP) 800-53 Security Controls; and
- Plan of Action and Milestones Process.

Scope and Methodology

Our 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 HRLOB officials responsible for EHRIDW, including IT security controls in place as of February 2009.

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 objectives.

To accomplish our objective, we interviewed representatives of OPM's HRLOB office and other program officials with EHRIDW 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 EHRIDW 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 EHRIDW system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM IT Security Policy;
- 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;
- NIST SP 800-12, An Introduction to Computer Security;
- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems;

- NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems;
- NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems;
- NIST SP 800-60 Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories;
- Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems; and
- Other criteria as appropriate.

In conducting the audit, we relied to varying degrees on computer-generated data. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. However, nothing came to our attention during our audit testing utilizing the computer-generated data to cause us to doubt its reliability. We believe that the data was sufficient to achieve the audit objectives. Except as noted above, the audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States.

The audit was performed by the OPM Office of the Inspector General, as established by the Inspector General Act of 1978, as amended. The audit was conducted from January through March 2009, in OPM's Washington, D.C. office.

Compliance with Laws and Regulations

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

Results

This section details the results of our audit of EHRIDW.

I. Self-Assessment

FISMA requires that IT security controls of each major application owned by a Federal agency be tested on an annual basis. In September 2008, an independent contractor tested the degree to which the management, operational, and technical controls outlined in NIST SP 800-53 have been implemented for EHRIDW (see section IV, below). Therefore, an internal self-assessment of these controls was not required in fiscal year (FY) 2008.

The OIG will verify that a self-assessment of NIST SP 800-53 controls is conducted for this system during FY 2009 as part of the general FISMA audit process.

II. Risk Assessment

An effective risk management process is an important component of a successful IT security program. NIST defines risk management as "the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level." NIST SP 800-30, Risk Management Guide for Information Technology Systems, offers a systematic approach for conducting risk assessments that includes the following nine steps:

- System Characterization;
- Threat Identification;
- Vulnerability Identification;
- Control Analysis;
- Likelihood Determination;
- Impact Analysis;
- Risk Determination;
- Control Recommendations; and
- Results Documentation.

A risk assessment was performed for EHRIDW by a contracted vendor in November 2008 that encompassed each of the elements outlined above.

In addition, a privacy impact assessment (PIA) was completed and signed for EHRIDW in November 2008. A PIA is used to ensure no collection, storage, access, use, or dissemination of personally identifiable information occurs that is not needed or permitted.

III. Information System Security Plan

The completion of an information system security plan (ISSP) is a requirement of OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources. The

EHRIDW ISSP was developed in accordance with NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems.

The ISSP for EHRIDW was prepared in accordance with the format and methodology outlined in NIST SP 800-18, and contained all major elements suggested by the guidance. The EHRIDW ISSP was completed by a contracted vendor, and was finalized in November 2008.

IV. Independent Security Test and Evaluation

A security test and evaluation (ST&E) was completed for the EHRIDW during September 2008 as part the system's FY 2009 certification and accreditation (C&A) process. The ST&E was conducted by Carson Associates, a company independent of OPM and the DOI NBC that hosts EHRIDW. The OIG verified that the test included a review of the appropriate management, operational, and technical controls required for a system with a "high" security categorization according to NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems.

Several NIST SP 800-53 controls were identified by Carson Associates as not applicable to the EHRIDW certification and accreditation. Carson Associates stated that these controls related to the hardware infrastructure maintained by the NBC, and therefore referred to the NBC C&A package for an assessment of these controls. The OIG evaluated the appropriateness of deferring these controls to the NBC, and did not disagree with Carson Associate's assessment.

In addition, several NIST SP 800-53 controls are related to agency-level policy and procedure requirements. When reviewing these controls, Carson Associates referred to the C&A package for the Electronic Official Personnel Folder (eOPF) application, which in turn referred to the relevant OPM IT security policy or procedure posted on OPM's internal web site. However, several of the policies referenced in the eOPF ST&E are extremely outdated, and the OIG believes that this represents a security weakness to any IT system that is subject to the guidance outlined in these documents. The maintenance of these policies and procedures is the responsibility of OPM's CIS. The OIG recommended in its FY 2008 FISMA audit report that these documents be updated, and therefore will not include this weakness as an audit finding in this report. However, HRLOB should evaluate the impact that any outdated information contained in these policies has on the security controls of EHRIDW.

The remaining NIST SP 800-53 controls were within the scope of the ST&E and Carson Associates determined whether each control was satisfied or not satisfied. Carson Associates presented a copy of the evaluation results to HRLOB, and helped the program office incorporate the identified weaknesses into the EHRIDW risk assessment.

V. Certification and Accreditation

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, states that certification is a comprehensive assessment that attests that a system's security controls are meeting the security requirements of that system, and accreditation is the official management decision to authorize operation of an information system and accept its risks. EHRIDW was certified and accredited on November 20, 2008, in accordance with NIST SP 800-37 requirements.

OPM's Certifying Official and IT security officer evaluated the security-related documentation that HRLOB provided in the certification package. The Certifying Official stated that the requirements for certification have been satisfied and suggested that the program office determine whether it is appropriate to formally accept certain risks identified during the C&A process.

The certification package was also reviewed by the Director of HRLOB, who was acting as the system's Authorizing Official. The Authorizing Official reviewed the security controls that have been implemented for the system, weighed the remaining residual risks against the operational requirements, and granted a three year Authorization to Operate to the EHRIDW major application.

VI. Contingency Planning

NIST SP 800-34, Contingency Planning Guide for IT Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. The OPM IT security policy requires that OPM general support systems and major applications have viable and logical disaster recovery and contingency plans, and that these plans are annually reviewed, tested, and updated.

The EHRIDW is hosted at the DOI NBC. In the event of a disaster, the NBC will perform all tasks associated with restoring communications, network infrastructure, servers, and applications. The OPM/HRLOB Operations Team has been assigned the responsibility to provide oversight, guidance, application-specific configurations, and application functionality testing during the disaster recovery process.

The contingency plan developed for EHRIDW has been tested and reviewed in accordance with NIST SP 800-34 by both the NBC and HRLOB. The plan addresses all of the key elements outlined in the NIST guidance.

VII. Federal Information Processing Standards Publication 199 Analysis

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, requires the development of standards for categorizing information and information systems to ensure that the appropriate levels of information security controls are implemented. NIST SP 800-60 Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories, provides additional guidance for

understanding the security objectives and impact levels identified in FIPS 199 by defining information types and determining each category's impact.

A security categorization and analysis was performed for EHRIDW that was based on both FIPS 199 and NIST SP 800-60 Volume II. The FIPS 199 analysis considered the potential level of impact (*low, moderate, high*) that would result from a loss of confidentiality, integrity, or availability of each of the information types. The OIG determined that this evaluation was adequate and agrees with the overall security categorization of *high* for EHRIDW.

VIII. NIST SP 800-53 Evaluation

NIST SP 800-53 provides guidance for implementing a variety of security controls for information systems supporting the Federal government. These controls are organized into three classes (management, operational, and technical). The OIG tested a subset of these controls for EHRIDW as part of this audit, including:

- AC-2: Account Management
- AC-7: Unsuccessful Login Attempts
- AC-11: Session Lock
- AC-13: Supervision and Review
- AU-2: Auditable Events
- AU-6: Audit Monitoring
- CM-3: Configuration Change Control
- CM-4: Monitoring Configuration Changes
- IA-5: Authenticator Management
- IR-2: Incident Response Training
- IR-5: Incident Monitoring
- IR-6: Incident Reporting
- RA-5: Vulnerability Scanning

These controls were evaluated by interviewing individuals with EHRIDW security responsibilities, reviewing documentation and system screenshots provided by HRLOB, and tests conducted on the system directly by the OIG.

Although the majority of NIST SP 800-53 controls appeared to be implemented for EHRIDW, several tested controls related to system auditing [redacted] and incident response [redacted] had not been implemented for this system. These control weaknesses were previously identified by HRLOB, and were appropriately included in the EHRIDW plan of action and milestones (POA&M). However, these POA&M items are over 120 days old and should be considered a high priority for HRLOB.

The OIG determined that one control, [redacted] has not been implemented and is not included on the EHRIDW POA&M. In prior years, HRLOB periodically evaluated the appropriateness of active EHRIDW user accounts [redacted]. However, this process no longer appears to be in place, as it has been over one year since the last review of active user accounts. Failure to routinely audit user accounts for appropriateness increases the risk that unauthorized individuals can access sensitive data on the system.

Recommendation 1

We recommend that HRLOB routinely audit active EHRIDW user accounts for appropriateness.

HRLOB Response:

"The Program Office concurs with this recommendation. . . . In response to the OIG's recommendation, the Program Office will ensure that it conducts reviews of active user accounts every six months as suggested in the Risk Assessment and documented in the POA&M so that the risk of unauthorized access to sensitive system data is reduced. The Program Office expects to have this in place by August 1, 2009."

IX. Plan of Action and Milestones Process

A POA&M is a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for IT security weaknesses. OPM has implemented an agency-wide POA&M process to help track known IT security weaknesses associated with the agency's information systems.

HRLOB submitted a current POA&M to OPM's CIS in November 2008. The OIG evaluated the following aspects of this POA&M:

Prioritization of Weaknesses

HRLOB uses the POA&M template provided by OPM's CIS to track security control weaknesses of EHRIDW. This template facilitates the prioritization of POA&M weaknesses, and HRLOB appears to be prioritizing its weaknesses per OPM policy and FISMA requirements.

Proof of Closure

The EHRIDW POA&M indicates that several security weaknesses were recently corrected and the POA&M item was closed. The OIG evaluated the "proof of closure" documentation that was submitted to OPM's CIS/CIO at the time the POA&M item was closed.

We requested proof of closure evidence for a sample of six POA&M items closed between December 31, 2007 and January 14, 2009. Of the six items requested, the OIG was only provided adequate proof of closure documentation for four of the POA&M items. Prior to June 2008, OPM's CIS/CIO did not have a well defined process for documenting POA&M proof of closure; this weakness was documented in the OIG's FY 2008 FISMA report. The four items that were missing were closed before June 2008, and the two that were provided were closed after June 2008. The OIG believes that this indicates that controls related to documenting proof of closure are currently in place for EHRIDW. As part of the FY 2009 general FISMA audit, OIG will verify that HRLOB continues to submit proof of closure documentation to CIS/CIO.

Including All Identified Weaknesses in POA&M

As mentioned in section IV, above, Carson Associates conducted an independent ST&E of the NIST SP 800-53 controls in place for EHRIDW. Carson identified at least 40 controls that were not fully implemented on the EHRIDW. A copy of the test results were presented to the HRLOB program office, and the results were incorporated into the EHRIDW risk assessment.

However, none of the weaknesses identified by Carson were included on the FY 2009 first quarter EHRIDW POA&M (dated November 1, 2008). This was brought to the attention of HRLOB during the fieldwork phase of this audit. In February 2009, HRLOB submitted an updated copy of the EHRIDW POA&M to the OIG, and we verified that the security weaknesses identified during the ST&E were now included in the POA&M.

The OIG is not aware of any other recent security assessments of EHRIDW that could lead to the identification of potential POA&M items.

Nothing came to our attention during this evaluation to indicate that there are any current weaknesses in HRLOB's management of POA&Ms.

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], Auditor-in-Charge
- [redacted], Information Technology Auditor

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of Modernization
and Human Resources
Line of Business

MEMORANDUM FOR [redacted]
Chief, Information Systems Audits Group

FROM: [redacted] 4/10/2009
Program Director, Enterprise Human Resources In[redacted]n
Human Resources Line of Business

Subject: Program Office Response to OIG Report Number 4A-HR-00-09-033, "Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Enterprise Human Resources Integration Data Warehouse"

Thank you for the opportunity to comment on 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 Enterprise Human Resources Integration Data Warehouse."

The Human Resources Line of Business (HRLOB) Enterprise Human Resources Integration (EHRI) Program Office has reviewed the report and agrees with the findings, conclusions, and recommendations presented. The Program Office is committed to resolving all outstanding IT security-related issues in a timely manner. Specifically, the Program Office will take the following actions to address the following OIG recommendation:

Recommendation 1: The OIG recommends that HRLOB routinely audit active EHRI Data Warehouse (DW) user accounts for appropriateness.

The Program Office concurs with this recommendation. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security control AC-2 that corresponds to this recommendation was identified as "partially satisfied" during security controls testing on August 28, 2008. Consequently, the EHRI DW Risk Assessment, dated November 19, 2008, identified a medium-risk vulnerability related to this control, and the vulnerability was added to the EHRI DW Plan of Action and Milestones (POA&M) as Item M37. To address this vulnerability, the Risk Assessment recommendation states that EHRI should make use of an automated process to review EHRI DW user accounts and fully document how it reviews EHRI DW accounts every six months. This documentation should include details on how access authorization forms are kept up-to-date and how authorization forms are kept in sync with actual system rights and privileges. In response to the OIG's recommendation, the Program Office will ensure that it conducts reviews of active user accounts every six months as suggested in the Risk Assessment and documented in the POA&M so that the risk of unauthorized access to sensitive system data is reduced. The Program Office expects to have this in place by August 1, 2009.

cc: Janet L. Barnes
Deputy Associate Director
Center for Information Services and Chief Information Officer

[redacted]
Information Technology Specialist
Center for Information Services

David M. Cushing
Deputy Chief Financial Officer

[redacted]
Human Resources Line of Business