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 ANNUITY ROLL SYSTEM FY 2010

Report No. 4A-CF-00-10-047

Date: November 22, 2010

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

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 ANNUITY ROLL SYSTEM FY 2010

WASHINGTON, D.C.

Report No. 4A-CF-00-10-047

Date: 11/22/2010

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 ANNUITY ROLL SYSTEM FY 2010

WASHINGTON, D.C.

Report No. 4A-CF-00-10-047

Date: 11/22/2010

This final audit report discusses the results of our review of the information technology security controls of the U.S. Office of Personnel Management's (OPM) Annuity Roll System (ARS). Our conclusions are detailed in the "Results" section of this report.

ARS is one of OPM's 43 critical IT systems, and is comprised of multiple sub-applications that contain detailed records of annuitants and their survivors and forms the basic pay records for disbursing retirement benefits. Although the OIG agrees that it is appropriate for many of the ARS applications to be grouped together as a single "system," several applications have distinct hardware/software infrastructures and security control requirements, support different user groups and business processes, and are supported by several separate system administrators. Therefore, we believe that the ARS subsystems should be divided into at least four major applications:

1. Federal Annuity Claim Expert System (FACES)
2. FEHB 2000
3. Coverage Determination Application (CDA) and Electronic Individual Retirement Record Data Capture Closeout Solution (E-IRR)
4. The 37 remaining applications

In addition to the concerns related to the grouping of the ARS sub-applications, the OIG documented the following opportunities for improvement:

- The information system security plan for ARS does not contain several critical elements required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18;
- The ARS Privacy Impact Assessment (PIA) is missing several elements required by OPM's PIA Guide. In addition, there is no evidence that the ARS PIA has been reviewed by the system owner on an annual basis, as required by OMB; and,
- [redacted]

The OIG also reviewed several elements of the ARS security program that appear to be in full FISMA compliance:

- A security certification and accreditation (C&A) of ARS was completed in April 2009 and appears to be in compliance with NIST SP 800-37;
- The security categorization of ARS appears to be consistent with the guidance of Federal Information Processing Standard 199, and the OIG agrees with the categorization as a moderate risk system;
- A risk assessment was conducted for ARS in 2009 that addresses all of the required elements outlined in relevant NIST guidance;
- The system security controls of ARS were appropriately tested as part of the C&A process;
- The ARS contingency plan contains the majority of elements required by NIST SP 800-34 guidelines; and,
- The ARS Plan of Action and Milestones (POA&M) follows the format of the OPM POA&M guide, and has been routinely submitted to the Office of the Chief Information Officer for evaluation.

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) Annuity Roll System (ARS).

Background

ARS is one of OPM's 43 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.

OPM's Retirement and Benefits Office (RBO) has been designated with ownership of ARS. ARS is comprised of multiple subsystems that contain detailed records of federal annuitants and their survivors and forms the basic pay records for disbursing retirement benefits. ARS applications reside on OPM's enterprise server mainframe and Local Area Network / Wide Area Network (LAN/WAN) environments.

Objectives

Our overall objective was to perform an evaluation of security controls for ARS to ensure that RBO officials have implemented IT security policies and procedures in accordance with standards established by OPM's Chief Information Officer (CIO).

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 security program elements have been implemented for ARS, including:

- Certification and Accreditation Statement;
- FIPS 199 Analysis;
- Information System Security Plan;
- Risk Assessment;
- Independent Security Control Testing;
- Security Control Self-Assessment;

- Contingency Planning and Contingency Plan Testing;
- Privacy Impact Assessment;
- Plan of Action and Milestones Process; and,
- NIST Special Publication (SP) 800-53 Security Controls.

Scope and Methodology

This performance audit was conducted in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures that we considered necessary. The audit covered FISMA compliance efforts of RBO and CIO officials responsible for ARS, including IT security controls in place as of May 2010.

We considered the ARS 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 objectives, we interviewed representatives of OPM's RBO program office and other program officials with ARS 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 were functioning as required.

Details of the security controls protecting the confidentiality, integrity, and availability of ARS 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 ARS system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Security and Privacy Policy Volume 1 and Volume 2;
- 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 3, 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) Publication 199, Standards for Security Categorization of Federal Information and Information Systems;
- FIPS Publication 200, Minimum Security Requirements for 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 March through May 2010 in OPM's Washington, D.C. office.

Compliance with Laws and Regulations

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

Results

I. Applications Included in the Annuity Roll System

OPM's Retirement Operations program within the RBO division provides Federal employees, retirees, and their families with retirement benefits and services. ARS is comprised of multiple subsystems that contain detailed records of annuitants and their survivors and forms the basic pay records for disbursing retirement benefits.

The ARS Information System Security Plan lists 41 subsystems that comprise the ARS major application. Thirty-seven of the ARS subsystems reside in OPM's Enterprise Server Environment (ESI), [redacted] [redacted] [redacted] Two additional subsystems, Coverage Determination Application (CDA) and Electronic Individual Retirement Record Data Capture Closeout Solution (E-IRR), also reside on OPM's mainframe, but are housed within [redacted] All systems on OPM's mainframe [redacted] are managed by the agency's Data Center Group (DCG). The final two systems, FEHB 2000 and Federal Annuity Claim Expert System (FACES), reside on [redacted] respectively. These [redacted] are part of OPM's LAN/WAN infrastructure, managed by the agency's Network Management Group (NMG).

OPM's inventory of information systems lists all 41 ARS applications as a single major application. Although all of these applications share many of the same managerial and operational security controls, they have distinct hardware/software infrastructures and security control requirements, support different user groups and business processes, and are supported by several separate system administrators. Therefore, we believe that the ARS subsystems should be divided into at least four major applications:

1. FACES ([redacted])
2. FEHB 2000 ([redacted] [redacted] [redacted])
3. CDA and E-IRR [redacted])
4. The 37 remaining applications [redacted])

NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, provides guidance for appropriately defining information system boundaries and grouping systems on an agency's system inventory. Although the NIST guide does allow agencies flexibility in defining an information system, it also states that grouped information systems should reside in the same general operating environment and have essentially the same operating characteristics and security needs.

Each of four groups of ARS subsystems is housed on different operating platforms that have unique security vulnerabilities. In order to adequately manage these vulnerabilities, ARS must assess the risks of all four groups individually, develop a customized and in-depth security approach tailored to each environment, and assign security responsibility to the appropriate user groups and system administrators. Without this customized approach, there is a risk that security controls will not adequately protect against the threats and vulnerabilities of each platform.

Recommendation 1

We recommend that the RBO work with OPM's CIO to classify the current ARS subsystems as appropriately grouped major applications on OPM's system inventory.

RBO Response:

"We concur with this recommendation. The Federal Annuity Claims Expert System (FACES) has been separated in the Agency's Master Inventory of FISMA systems. In the future, the certification and accreditation assessments of the Annuity Roll Systems will be grouped as follows:

1. ***FACES ([redacted]);***
2. ***FEHB 2000 ([redacted]);***
3. ***CDA and E-IRR ([redacted]); and,***
4. ***Remaining Applications ([redacted]);***

Since the annual testing for Fiscal Year 2010 has been completed by an independent tester, we can segment the documentation only to the extent possible for this Fiscal Year. When the continuous monitoring is completed for Fiscal Year 2011, the documentation will be separated no later than September 30, 2011."

OIG Reply:

We acknowledge the steps that the RBO has taken to address this recommendation. As part of the audit resolution process, we recommend that the RBO provide OPM's Office of Internal Oversight and Compliance (IOC) with appropriate supporting documentation indicating that OPM's system inventory reflects the four groupings of ARS subsystems, and that each group is subject to its own Certification and Accreditation (C&A).

II. Certification and Accreditation Statement

A security C&A of ARS was completed in April 2009. The Bureau of Public Debt (BPD) was contracted by OPM to prepare the C&A package for ARS. The ARS security statement was signed by OPM's former acting IT Security Officer, who recommended that the system be authorized to operate. The accreditation statement was signed by the Deputy Associate Director for OPM's Center for Retirement and Insurance Services (now RBO).

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, provides guidance to Federal agencies in meeting security accreditation requirements. The ARS C&A appears to have been conducted in compliance with NIST guidance. Although we believe the scope of the current C&A appeared to adequately cover all 41 subsystems that comprise ARS, we believe that a separate C&A must be conducted on each of the four groups of ARS subsystems in order to adequately manage the security risks and vulnerabilities of each unique environment (see Section I, above).

III. FIPS 199 Analysis

FISMA requires Federal agencies to categorize all Federal information and information systems in order to provide appropriate levels of information security according to a range of risk levels. FISMA also establishes three security objectives for information and information systems (confidentiality, integrity, and availability).

FIPS Publication 199 defines three levels of potential impact (low, moderate, and high) on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). ARS is categorized with a moderate impact level for confidentiality, moderate for integrity, moderate for availability, and an overall categorization of moderate.

The security categorization of ARS appears to be consistent with the guidance of FIPS 199, and the OIG agrees with the categorization of moderate.

IV. Information System Security Plan

FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, specifies the security requirements that must be implemented on all federal information systems. Federal agencies must implement the minimum security requirements defined in FIPS Publication 200 through the use of the security controls outlined in NIST SP 800-53, Recommended Security Controls for Federal Information Systems. NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in an information systems security plan (ISSP) for each system, and provides guidance for doing so.

The ARS ISSP contains the majority of the elements outlined in the NIST guide, including:

- Information System Name/Title;
- Information System Categorization;
- Information System Owner;
- Authorizing Official;
- Assignment of Security Responsibility;
- Information System Operational Status;
- Information System Type;
- General System Description/Purpose;
- System Environment;
- Related Laws/Regulations/Policies; and
- Minimum Security Controls.

The ARS ISSP also contains a section that describes the system's external interfaces with other federal agencies. However, based on the information within the ISSP, the Memorandum of Understanding (MOU) related to two of these interconnections has expired.

In addition, no details of these interconnections are provided within the ISSP, as required by NIST 800-18 Revision 1.

Recommendation 2

We recommend that the RBO implement active MOUs for any interconnections between ARS and another federal agency.

Recommendation 3

We recommend that all interconnections between ARS and a system owned by another agency be described in the ISSP, with details including:

- Name of the system;
- Organization;
- Type of interconnection;
- Authorizations for interconnection (MOU/MOA, ISA);
- Date of agreement;
- FIPS 199 category;
- Certification and accreditation status of system; and,
- Name and title of authorizing official(s).

RBO Response:

"We concur with these recommendations.

We have renegotiated the computer matching agreement with the Social Security Administration (SSA) which enables the Social Security Administration to identify individuals to determine their eligibility for Medicare Savings Programs and subsidized Medicare prescription drug coverage and enables them to identify these individuals to the States. The dates for this matching program are from April 2, 2010 through September 30, 2011.

We have also renegotiated the computer matching agreement with the Social Security Administration which allows the U.S. Office of Personnel Management (OPM) to match the Social Security Administration's data with OPM's records on disability retirees under age 60, disabled adult child survivors, certain retirees in receipt of a supplemental benefit under the Federal Employees Retirement System (FERS), and certain annuitants receiving a discontinued service retirement under the Civil Service Retirement System (CSRS). By law, these annuitants and survivors are limited in the amount they can earn. OPM will use the SSA data to determine continued eligibility for the civil service annuity being paid. The dates for this matching program are from May 29, 2010 through November 29, 2011.

We will develop the additional recommended information regarding the certification and accreditation of the interconnected systems no later than February 28, 2011."

OIG Reply - Recommendation 2:

We acknowledge the steps that the RBO has taken to address this recommendation. As part of the audit resolution process, we recommend that the RBO provide OPM's IOC with appropriate supporting documentation of the renegotiated matching agreements with the Social Security Administration and the implementation of active MOUs for any interconnections between ARS and another Federal agency.

OIG Reply - Recommendation 3:

We acknowledge the steps that the RBO intends to take to address this recommendation. As part of the audit resolution process, we recommend that the RBO provide OPM's IOC with an updated ISSP that contains the information outlined in Recommendation 3.

V. Risk Assessment

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

As part of the C&A process, BPD conducted a vulnerability assessment of ARS and evaluated the risk of each vulnerability in accordance with NIST SP 800-30 standards. BPD identified 25 vulnerabilities during this assessment, and for each one documented:

- Vulnerability description;
- Threat Source;
- Existing Controls;
- Likelihood, Impact, and Risk Rating; and,
- Control Recommendations.

Although we believe the scope of the current risk assessment appeared to adequately cover all 41 subsystems that comprise ARS, we believe that a separate risk assessment must be conducted on each of the four groups of the ARS subsystems in order to adequately manage the security risks and vulnerabilities of each unique environment (see Section I, above).

VI. Security Control Testing

FISMA requires that IT security controls of each major application owned by a Federal agency be tested on an annual basis.

A security test and evaluation (ST&E) was completed for ARS during June 2009 as part the system's FY 2009 C&A process. The ST&E was conducted by BPD. The OIG verified that the test included a review of the appropriate management, operational, and technical controls required for a system with a "moderate" security categorization according to NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems.

Several NIST SP 800-53 controls were identified by BPD as not applicable to the ARS certification and accreditation. The remaining NIST SP 800-53 controls were deemed within the scope of the ST&E and BPD determined whether each control was satisfied or not satisfied. The ST&E reported 16 findings and corresponding recommendations, each of which was appropriately documented in the ARS POA&M.

As of September 30, 2010 the OIG was not provided with evidence that the ARS security controls were tested during FY 2010. This is reflected as a finding in the OIG's FY 2010 FISMA audit report.

Although we believe the scope of the current risk assessment appeared to adequately cover all 41 subsystems that comprise ARS, we believe that a separate risk assessment must be conducted on each of the four groups of ARS subsystems in order to adequately manage the security risks and vulnerabilities of each unique environment (see Section I, above).

VII. Contingency Planning and Contingency Plan Testing

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 be annually reviewed, tested, and updated.

a) Contingency Plan

The ARS contingency plan discusses the procedures, responsibilities, and resources that are required for a successful recovery of the system if it were to become inoperable. The ARS contingency plan contains the majority of elements required by NIST SP 800-34 guidelines, including:

- System background information;
- Concept of operations;
- Notification/activation phase;
- Recovery operations; and,
- Procedures to return to normal operations.

b) Contingency Plan Test

ARS is housed on a mainframe and servers maintained by OPM's CIO. The CIO conducts a test of the enterprise server [redacted] and LAN/WAN [redacted] environments on an annual basis. The OIG verified that contingency plan tests were conducted for the enterprise server during FY 2010.

VIII. Privacy Impact Assessment

The E-Government Act of 2002 requires agencies to perform a screening of Federal information systems to determine if a Privacy Impact Assessment (PIA) is required for that system. OMB Memorandum M-03-22 outlines the necessary components of a PIA. The purpose of the assessment is to evaluate any vulnerabilities of privacy in information systems and to document any privacy issues that have been identified and addressed.

In 2006, OPM issued a "PIA Guide" to assist system owners in conducting assessments. A PIA was completed for ARS in July 2007 in accordance with the PIA Guide. However, OPM's PIA Guide is missing several elements required by OMB Memorandum M-032-022. Consequently, the ARS PIA is missing these elements as well.

OMB Memorandum M-032-022 states that PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA. In addition, PIAs for major applications should reflect more extensive analyses of: consequences of collection and flow of information; the alternatives to collection and handling as designed; the appropriate measures to mitigate risks identified for each alternative; and, the rationale for the final design choice or business process.

In addition, there is no evidence that the ARS PIA has been reviewed by the system owner on an annual basis, as required by OMB.

Recommendation 4

We recommend that the RBO conduct a new PIA for ARS that includes all of the required elements from OMB Memorandum M-03-22.

Recommendation 5

We recommend that the RBO review the ARS PIA on an annual basis and submit evidence of this review to the CIO.

RBO Response:

"We concur with these recommendations.

In Fiscal Year 2010, we completed and received approval from the Chief Information Officer of Privacy Threshold Analyses for the systems identified in the FISMA inventory, demonstrating the annual review of the Privacy Impact Assessments, using guidance that was issued by the Agency in April 2010.

We are also completing Privacy Impact Assessments in accordance with the new Agency guidance that was issued in April 2010. We plan to complete the new Privacy Impact Assessments to be completed for all of the systems in the inventory no later than January 31, 2011."

OIG Reply - Recommendation 4:

We acknowledge the steps that the RBO intends to take to address this recommendation. As part of the audit resolution process, we recommend that the RBO provide OPM's IOC with appropriate supporting documentation that a new PIA has been conducted for each of the four new groupings of ARS subsystems.

OIG Reply - Recommendation 5:

We acknowledge the steps that the RBO has taken to address this recommendation. As part of the audit resolution process, we recommend that the RBO provide OPM's IOC with evidence that the ARS PIAs are reviewed on an annual basis.

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 efforts to remediate 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 OIG evaluated the ARS POA&M and verified that it follows the format of OPM's template, and has been routinely submitted to the CIO for evaluation. We also determined that the POA&M contained action items for all security weaknesses identified through various security control tests and audits.

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

X. 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. The OIG tested a subset of these controls for ARS as part of this audit, including:

- AC-2: Account Management
- AC-6: Least Privilege
- AC-7: Unsuccessful Login Attempts
- AC-11: Session Lock
- AC-13: Supervision and Review – Access Control
- AU-2: Auditable Events
- AU-3: Content of Audit Records
- CM-1: Configuration Management Policy and Procedures
- CM-2: Baseline Configuration
- CM-3: Configuration Change Control
- CM-6: Configuration Settings
- IA-2: Identification and Authentication
- IA-5: Authenticator Management
- PL-4: Rules of Behavior
- PS-4: Personnel Termination
- RA-5: Vulnerability Scanning

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

Although it appears the RBO and the CIO have successfully implemented the majority of NIST SP 800-53 security controls for ARS, several tested controls were not fully satisfied:

a) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation 6

We recommend that the RBO routinely [redacted]

RBO Response:

"We partially concur with this recommendation.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

OIG Reply:

We acknowledge the steps that the RBO is taking [redacted]

[redacted]

Recommendation 7

We recommend that the RBO periodically [redacted]

RBO Response:

"We concur with this recommendation. [redacted] *Effective July 27, 2010, all of the system administrators for the above systems began to receive the report."*

OIG Reply:

[redacted]

b) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation 8

We recommend that the RBO develop [redacted]

Recommendation 9

We recommend that FACES, FEHB 2000, CDA, and E-IRR be modified to [redacted]

Recommendation 10

We recommend that the RBO [redacted]

RBO Response:

"We partially concur with these recommendations.

[redacted]

[redacted]

[redacted]

. . .

[redacted]

[redacted]

[redacted]

[redacted]

OIG Reply Recommendation 8:

We acknowledge the steps that the RBO intends to take to address this recommendation. As part of the audit resolution process, we recommend that the RBO provide OPM's IOC with appropriate supporting documentation of its efforts to [redacted]

OIG Reply Recommendation 9:

We acknowledge the steps that the RBO is taking to [redacted]

OIG Reply Recommendation 10:

We acknowledge the steps that the RBO is taking to improve the [redacted]

c) Baseline configuration (CM-2)

The FACES application is housed on a [redacted]. Although OPM has developed a standardized [redacted] configuration policy, the agency does not have a configuration policy for [redacted].

NIST SP 800-53 Revision 3 control CM-1 states that "The organization develops, disseminates, and periodically reviews/updates: . . . a. a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls."

Recommendation 11

We recommend that the RBO develop a configuration management policy for the [redacted].

RBO Response:

"We do not concur with this finding.

The FACES system currently functions utilizing a [redacted] baseline. The policy dictating the use of these baselines can be found on page 11 of the Information Security and Privacy Policy Volume 1, which may be found at the following reference: [redacted]

OIG Reply:

The OIG reviewed the documentation provided in response to the draft audit report and determined that a [redacted] security configuration baseline has been developed for OPM. However, during the fieldwork phase of this audit, the ARS SQL Server database administrator (DBA) stated that he was not aware of a standard SQL Server baseline configuration at OPM, and that he configured the FACES database based on his experience and industry best-practices.

The original recommendation 11 has been satisfied, and is updated to the following:

Recommendation 11 (update)

We recommend that the RBO compare the current database configuration to OPM baseline and implement any necessary changes. We also recommend that the RBO implement procedures to routinely monitor and audit server configurations to ensure ongoing compliance with [redacted] server configuration baseline.

d) Configuration Settings (CM-6)

[redacted]

[redacted]

Recommendation 12

We recommend that the [redacted]

RBO Response:

"We concur with this recommendation. [redacted]

[redacted]

[redacted]

[redacted]

OIG Reply:

We acknowledge the steps that the RBO intends to take to address this recommendation. As part of the audit resolution process, we recommend that the RBO provide OPM's IOC with appropriate supporting documentation [redacted].

e) Authenticator Management (IA-5)

Procedures for managing passwords for FEHB 2000 user accounts could be improved.

[redacted]

[redacted]

Recommendation 13

We recommend that the FEHB 2000 application be modified [redacted].

RBO Response:

"We concur with this finding. We plan for implementation no later than May 31, 2011."

OIG Reply:

We acknowledge the steps that the RBO intends to take to address this recommendation. As part of the audit resolution process, we recommend that the RBO provide OPM's IOC with appropriate supporting documentation of its efforts to modify the FEHB 2000 application to force users to change their passwords on a periodic basis.

Major Contributors to this Report

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

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

Appendix

OPM Response to the Inspector General's Report of the Audit of Information Technology Security Controls for the Annuity Roll Systems

August 9, 2010

MEMORANDUM FOR [redacted] [redacted] [redacted]., Chief
Information Systems Audit Group
Inspector General

FROM: William Zielinski, Associate Director
Retirement and Benefits

SUBJECT: Audit of Information Technology Security Controls of the U.S. Office of Personnel Management's Annuity Roll Systems.

Summary of OPM Position

We have reviewed your draft audit report on OPM's Information Technology Security Controls for the Annuity Roll Systems and are in concurrence with several of the findings and recommendations identified in the report. We recognize that even the most well run programs can benefit from an external evaluation and we appreciate the input of the Office of the Inspector General as we continue to work to enhance our security controls for the Annuity Roll Systems. Specific responses to your recommendations are provided below.

Response to Recommendations

For each Finding and Recommendation identified in the draft audit report, a response is included below.

FINDING: Each of four groups of ARS subsystems is housed on different operating platforms that have unique security vulnerabilities. In order to adequately manage these vulnerabilities, ARS must assess the risks of all four groups individually; develop a customized and in-depth security approach tailored to each environment, and assign security responsibility to the appropriate user groups and system administrators. Without this customized approach, there is a risk that security controls will not adequately protect against the threats and vulnerabilities of each platform.

RECOMMENDATION 1: We recommend that R&B work with OPM's CIO to classify the current ARS subsystems as appropriately grouped major applications on OPM's system inventory.

MANAGEMENT RESPONSE: We concur with this recommendation. The Federal Annuity Claims Expert System (FACES) has been separated in the Agency's Master Inventory of FISMA systems. In the future, the certification and accreditation assessments of the Annuity Roll Systems will be grouped as follows:

1. FACES [redacted]
2. FEHB 2000 [redacted]
3. CDA and E-IRR ([redacted]
4. Remaining Applications [redacted]

Since the annual testing for Fiscal Year 2010 has been completed by an independent tester, we can segment the documentation only to the extent possible for this Fiscal Year. When the continuous monitoring is completed for Fiscal Year 2011, the documentation will be separated no later than September 30, 2011.

FINDING: The ARS ISSP also contains a section that describes the system's external interfaces with with other federal agencies. However, based on the information within the ISSP, the Memorandum of Understanding (MOU) related to two of these interconnections has expired. In addition, no details of these interconnections are provided within the ISSP, as required by NIST 800-18 Revision 1.

RECOMMENDATION 2: We recommend that R&B implement active MOUs for any interconnections between ARS and another federal agency.

RECOMMENDATION 3: We recommend that all interconnections between ARS and a system owned by another agency be described in the ISSP, with details including:

- Name of the system;
- Organization;
- Type of interconnection;
- Authorizations for interconnection (MOU/MOA, ISA);
- Date of agreement;
- FIPS 199 category;
- Certification and accreditation status of system; and,
- Name and title of authorizing official(s).

MANAGEMENT RESPONSE: We concur with these recommendations.

We have renegotiated the computer matching agreement with the Social Security Administration (SSA) which enables the Social Security Administration to identify individuals to determine their eligibility for Medicare Savings Programs and subsidized

Medicare prescription drug coverage and enables them to identify these individuals to the States. The dates for this matching program are from April 2, 2010 through September 30, 2011.

We have also renegotiated the computer matching agreement with the Social Security Administration which allows the U.S. Office of Personnel Management (OPM) to match the Social Security Administration's data with OPM's records on disability retirees under age 60, disabled adult child survivors, certain retirees in receipt of a supplemental benefit under the Federal Employees Retirement System (FERS), and certain annuitants receiving a discontinued service retirement under the Civil Service Retirement System (CSRS). By law, these annuitants and survivors are limited in the amount they can earn. OPM will use the SSA data to determine continued eligibility for the civil service annuity being paid. The dates for this matching program are from May 29, 2010 through November 29, 2011.

We will develop the additional recommended information regarding the certification and accreditation of the interconnected systems no later than February 28, 2011.

FINDING: The OMB Memorandum states that PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA. In addition, PIAs for major applications should reflect more extensive analyses of: consequences of collection and flow of information; the alternatives to collection and handling as designed; the appropriate measures to mitigate risks identified for each alternative; and the rationale for the final design choice or business process.

In addition, there is no evidence that the ARS PIA has been reviewed by the system owner on an annual basis, as required by OMB.

RECOMMENDATION 4: We recommend that R&B conduct a new PIA for ARS that includes all of the required elements from OMB Memorandum M-03-22.

RECOMMENDATION 5: We recommend that R&B review the ARS PIA on an annual basis and submit evidence of this review to the CIO.

MANAGEMENT RESPONSE: We concur with these recommendations.

In Fiscal Year 2010, we completed and received approval from the Chief Information Officer of Privacy Threshold Analyses for the systems identified in the FISMA inventory, demonstrating the annual review of the Privacy Impact Assessments, using guidance that was issued by the Agency in April 2010.

We are also completing Privacy Impact Assessments in accordance with the new

Agency guidance that was issued in April 2010. We plan to complete the new Privacy Impact Assessments will be completed for all of the systems in the inventory no later than January 31, 2011.

FINDING: [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

MANAGEMENT RESPONSE: We partially concur with this recommendation.

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

RECOMMENDATION 7: [redacted]

[redacted]

FINDING: [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

RECOMMENDATION 8: We recommend that R&B develop [redacted]

RECOMMENDATION 9: We recommend that [redacted].

RECOMMENDATION 10: We recommend that R&B routinely [redacted]

MANAGEMENT RESPONSE: We partially concur with these recommendations.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

- [redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

FINDING: The FACES application is housed on a [redacted] supported by a Microsoft SQL database. Although OPM has developed a standardized [redacted] configuration policy, the agency does not have a configuration policy for [redacted] configuration policy.

NIST SP 800-53 Revision 2 control CM-1 states that "the organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls."

RECOMMENDATION 11: We recommend that R&B develop a configuration management policy for the [redacted] supporting FACES.

MANAGEMENT RESPONSE: We do not concur with this finding.

The FACES system currently functions utilizing a [redacted] [redacted] baseline. The policy dictating the use of these baselines can be found on page 11 of the Information Security and Privacy Policy Volume 1, which may be found at the following reference: http://theo.opm.gov/policies/ispp/isp_policy1.pdf.

FINDING: [redacted]

[redacted]

RECOMMENDATION 12: [redacted]

MANAGEMENT RESPONSE: We concur with this recommendation. [redacted]

[redacted]

FINDING: Procedures for managing passwords for FEHB 2000 user accounts could be improved.

[redacted]

[redacted]

RECOMMENDATION 13: We recommend that the FEHB 2000 application be modified to [redacted]

MANAGEMENT RESPONSE: We concur with this finding. We plan for implementation no later than May 31, 2011.

Attachments

cc:
Internal Oversight and Compliance
Other Internal OPM parties (as appropriate)