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 SERVICES ONLINE SYSTEM FY 2014

Report No. 4A-RI-00-14-018

Date: April 3,2014

--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 the 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.

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S SERVICES ONLINE SYSTEM
FY 2014

WASHINGTON, D.C.

Report No. 4A-RI-00-14-018

Date: April 3,2014

Michael R. Esser
Assistant Inspector General
for Audits

--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 the 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.

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

--

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S SERVICES ONLINE SYSTEM
FY 2014

WASHINGTON, D.C.

Report No. 4A-RI-00-14-018

Date: April, 3, 2014

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

Security Assessment and Authorization (SA&A)
An SA&A of SOL was completed in March 2011. We reviewed the authorization package for all required elements of an SA&A, and determined that the package contained all necessary documentation.

Federal Information Processing Standards (FIPS) 199 Analysis
The security categorization of SOL appears to be consistent with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 requirements, and we agree with the categorization of "moderate."

System Security Plan (SSP)
The SOL SSP contains the critical elements required by NIST SP 800-18 Revision 1.

Security Assessment Plan and Report

A security control assessment plan and report were completed in December 2010 and January 2011 for SOL as a part of the system's SA&A.

Security Control Self-Assessment

Retirement Services ensures that semi-annual security control self-assessments are conducted in accordance with OPM's continuous monitoring methodology.

Contingency Planning and Contingency Plan Testing

A contingency plan was developed for SOL that is in compliance with NIST SP 800-34 Revision 1, and the plan is tested annually.

Privacy Impact Assessment (PIA)

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

Plan of Action and Milestones (POA&M) Process

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

NIST SP 800-53 Revision 3 Evaluation

We evaluated the degree to which a subset of the IT security controls outlined in NIST SP 800-53 Revision 3 were implemented for SOL. We determined that all tested security controls appear to be in compliance with NIST SP 800-53 Revision 3 requirements.

Contents

Introduction

On December 17, 2002, President Bush signed into law the E-Government Act (P.L. 107-347), which includes Title III, the Federal Information Security Management Act (FISMA). It requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the Office of Management and Budget (OMB) the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In accordance with FISMA, we audited the information technology (IT) security controls related to the Office of Personnel Management's (OPM) Services Online (SOL) System.

Background

SOL is one of OPM's critical IT systems. As such, FISMA requires that the Office of the Inspector General (OIG) perform an audit of IT security controls of this system, as well as all of the agency's critical systems on a rotating basis.

The SOL system is a secure, web-based, self-service information system. Current or former employees of the Federal Government can find general and personal information about retirement benefits and make changes concerning their annuity payment through the SOL web site. Authorized SOL users can use this web site to start, change, or stop their Federal and State income tax withholdings, view/print Form 1099-R, change their mailing address, sign up for or change their account or financial institution for direct deposit of their annuity payment, make allotments to organizations, create checking or savings allotments, and view a monthly statement of their annuity. The system is owned by OPM's Retirement Services program office.

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

Objectives

Our objective was to perform an evaluation of the system's security controls to ensure that SOL officials have implemented IT security policies and procedures in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual (FISCAM) and OPM's Office of the Chief Information Officer (OCIO).

OPM's IT security policies require managers of all major information systems to complete a series of steps to (1) certify that their system's information is adequately protected and (2) authorize the system for operations. The audit objective was accomplished by reviewing the degree to which a variety of security program elements have been implemented for SOL, including:

- Security Assessment and Authorization;
- FIPS 199 Analysis;
- System Security Plan;
- Security Assessment Plan and Report;

- Security Control Self-Assessment;
- Contingency Planning and Contingency Plan Testing;
- Privacy Impact Assessment;
- Plan of Action and Milestones Process; and
- NIST Special Publication (SP) 800-53 Revision 3, Security Controls.

Scope and Methodology

This performance audit was conducted in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures that we considered necessary. The audit covered FISMA compliance efforts of officials responsible for SOL, including an evaluation of the IT security controls in place as of February 2014.

We considered the SOL 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 Retirement Services division and other individuals with SOL 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 SOL 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 SOL system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Technology Security Policy Volumes 1 and 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;
- The Federal Information System Controls Audit Manual;
- NIST SP 800-12, An Introduction to Computer Security;
- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-37 Revision 1, Guide for Applying Management Framework to Federal Information Systems;

- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations;
- NIST SP 800-60 Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories;
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities;
- Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems; and
- Other criteria as appropriate.

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

The audit was performed by the OPM Office of the Inspector General, as established by the Inspector General Act of 1978, as amended. The audit was conducted from November 2013 through February 2014 in OPM's Washington, D.C. office. This was our first audit of the security controls surrounding SOL.

Compliance with Laws and Regulations

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

Results

I. Security Assessment and Authorization

A Security Assessment and Authorization (SA&A) of SOL was completed in March 2011.

OPM's Chief Information Security Officer reviewed the SOL SA&A package and signed the system's authorization letter on March 9, 2011. The system's authorizing official signed the letter and authorized the continued operation of the system on March 10, 2011.

NIST SP 800-37 Revision 1 "Guide for Applying Management Framework to Federal Information Systems," provides guidance to federal agencies in meeting security accreditation requirements. The SOL SA&A appears to have been conducted in compliance with NIST requirements.

II. FIPS 199 Analysis

Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, requires federal agencies to categorize all federal information and information systems in order to provide appropriate levels of information security according to a range of risk levels.

NIST SP 800-60 Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories, provides an overview of the security objectives and impact levels identified in FIPS Publication 199.

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

III. System Security Plan

Federal agencies must implement on each information system the security controls outlined in NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations. NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in a System Security Plan (SSP) for each system, and provides guidance for doing so.

The SSP for SOL was created using the template outlined in NIST SP 800-18. The template requires that the following elements be documented within the SSP:

- System Name and Identifier;
- System Categorization;

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

We reviewed the SOL SSP and determined that it adequately addresses each of the elements required by NIST.

IV. Security Assessment Plan and Report

A Security Assessment Plan (SAP) and Security Assessment Report (SAR) were completed for SOL in December 2010 and January 2011 as a part of the system's SA&A process. The SAP and SAR were conducted by a contractor that was operating independently from Retirement Services. We reviewed the documents to verify that a risk assessment was conducted in accordance with NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments. We also verified that appropriate management, operational, and technical controls were tested for a system with a "moderate" security categorization according to NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations.

The SAP outlined the assessment approach, scanning authorization, and test methods. The SAR identified eight control weaknesses that were discovered as a result of a vulnerability assessment; six of those weaknesses have been remediated, and the remaining weaknesses were added to the SOL Plan of Action & Milestones (POA&M).

We also reviewed the Security Assessment results table that contained the detailed results of the NIST SP 800-53 Revision 3 controls testing. The table indicated that two controls were not fully satisfied.

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

V. Security Control Self-Assessment

OPM requires that the IT security controls of each major application owned by a federal agency be evaluated on a continual basis. In the years that an independent assessment is not being conducted as part of an SA&A, the system's owner must test a subset of security controls twice per year in accordance with OPM's continuous monitoring methodology.

We reviewed the SOL Continuous Monitoring Security Report that presents the results from the control assessments conducted in October 2012 and March 2013. The assessment included a review of the relevant management, operational, and technical security controls outlined in NIST SP 800-53 Revision 3. Nothing came to our attention to indicate that the security controls of SOL have not been adequately tested.

A fourth revision to NIST SP 800-53 was published in April 2013, and agencies are allowed one year to implement any new or modified NIST guidance. The POA&M for SOL includes NIST SP 800-53 Revision 4 gap analysis to determine if testing modifications are necessary for the fiscal year 2014 security controls tests.

VI. Contingency Planning and Contingency Plan Testing

NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. OPM's security policies require all major applications to have viable and logical disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

Contingency Plan

The SOL contingency plan documents the functions, operations, and resources necessary to restore and resume SOL operations when unexpected events or disasters occur. The SOL contingency plan closely follows the format suggested by NIST SP 800-34 Revision 1 and contains a majority of the suggested elements.

Contingency Plan Test

NIST SP 800-34 Revision 1 provides guidance for testing contingency plans and documenting the results. Contingency plan testing is a critical element of a viable disaster recovery capability.

A functional test of the SOL contingency plan was conducted in April 2013. The test involved recovering the SOL database at the off-site recovery location. The testing documentation contained an analysis and review of the results. We reviewed the testing documentation to determine if the test conformed to NIST 800-34 Revision 1 guidelines.

VII. Privacy Impact Assessment

FISMA 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.

Retirement Services completed an initial privacy screening or Privacy Threshold Analysis of SOL and determined that a PIA was required for this system. A PIA was conducted in March 2011 and approved by the system owner and CIO.

VIII. 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.

We evaluated the SOL POA&M and verified that it follows the format of OPM's standard template and has been loaded into Trusted Agent, the OCIO's POA&M tracking tool, for evaluation. Nothing came to our attention to indicate that there are any current weaknesses in the management of POA&Ms.

IX. NIST SP 800-53 Revision 3 Evaluation

NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, provides guidance for implementing a variety of security controls for information systems supporting the federal government. As part of this audit, we evaluated whether a subset of these controls had been implemented for SOL. We tested approximately 33 security controls outlined in NIST SP 800-53 Revision 3 that were identified as being system specific or a hybrid control. Controls identified as common or inherited were omitted from testing because another system or program office is responsible for implementing the control. We tested one or more controls from each of the following control families:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authorization
- Incident Response
- Media Storage
- Planning
- Risk Assessment
- System and Services Acquisition
- System and Communication Protection
- System and Information Integrity

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

We determined that all tested security controls appear to be in compliance with NIST SP 800-53 Revision 3 requirements.

Major Contributors to this Report

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

- [redacted], Group Chief
- [redacted], Auditor-In-Charge
- [redacted], IT Auditor

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Retirement Services

March 7, 2014

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

FROM: KENNETH J. ZAWODNY, Jr.
Associate Director
Retirement Services

SUBJECT: Inspector General Report No. 4A-RI-00-14-018 Information Technology Security Controls Audit of Services Online System

This memorandum is to acknowledge receipt of the Draft Audit Report of the Information Technology Security Controls Audit of Services Online System (Report No. 4A-RI-00-14-018). While Retirement Services appreciates the opportunity to provide comments on the draft report, we concur with the determination that all the tested security controls for Services Online were in compliance with NIST SP 800-53 Revision 3 requirements and therefore, we have no comments.