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 BENEFEDS AND FEDERAL LONG TERM CARE INSURANCE PROGRAM SYSTEMS FY 2014

Report No. 4A-RI-00-14-036

Date: August 19, 2014

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S BENEFEDS AND FEDERAL LONG TERM CARE INSURANCE PROGRAM SYSTEMS
FY 2014

WASHINGTON, D.C.

Report No. 4A-RI-00-14-036

Date: August 19, 2014

Michael R. Esser
Assistant Inspector General for Audits

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S BENEFEDS AND FEDERAL LONG TERM CARE INSURANCE PROGRAM SYSTEMS
FY 2014

WASHINGTON, D.C.

Report No. 4A-RI-00-14-036

Date: August 19, 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) BENEFEDS and Federal Long Term Care Insurance Program (FLTCIP) information systems. Our conclusions are detailed in the "Results" section of this report.

Security Assessment and Authorization (SA&A)

SA&A's were completed for BENEFEDS and FLTCIP in March 2013. We reviewed the authorization package for all required elements of an SA&A, and determined that both SA&As appear to have been conducted in compliance with National Institute of Standard and Technology (NIST) requirements.

Federal Information Processing Standards (FIPS) 199 Analysis

The security categorization of both the BENEFEDS and FLTCIP systems appears to be consistent with FIPS 199 and NIST Special Publication (SP) 800-60 requirements, and we agree with the categorization of "moderate."

System Security Plan (SSP)

We reviewed the BENEFEDS and FLTCIP SSPs and determined they adequately address each of the elements suggested by NIST.

Security Assessment Plan and Report

A security control assessment plan and report was completed for BENEFEDS and FLTCIP in July 2012 as a part of each system's SA&A.

Security Control Self-Assessment

We were provided with evidence that a security controls test was conducted in 2013 by an independent third-party. However, we are unable to verify that the assessment was conducted in accordance with OPM policy.

Contingency Planning and Contingency Plan Testing

The contingency plans for both BENEFEDS and FLTCIP closely follow the format suggested by NIST SP 800-34 Revision 1, and both systems have been tested in accordance with the published guidance.

Privacy Impact Assessment (PIA)

A privacy threshold analysis was completed for BENEFEDS and FLTCIP and determined that a PIA was required. A PIA was conducted in February 2013.

Plan of Action and Milestones (POA&M) Process

The BENEFEDS and FLTCIP POA&Ms follow the format of the OPM POA&M guide, and have been routinely submitted to the Office of the Chief Information Officer 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 was implemented for the BENEFEDS and FLTCIP systems. We determined that several controls could be improved.

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) BENEFEDS and Federal Long Term Care Insurance Program (FLTCIP) information systems.

Background

BENEFEDS and FLTCIP are two of OPM's critical IT systems. As such, FISMA requires that the Office of the Inspector General (OIG) perform audits of IT security controls for these systems, as well as all of the agency's systems, on a rotating basis.

The BENEFEDS and FLTCIP systems are both owned by OPM's Healthcare and Insurance Office (HI) and operated by a contractor, the Long Term Care Partners (LTCP) organization, located in Portsmouth, New Hampshire. The systems operate independently, but share many operational and security controls. Therefore, we have combined our audit findings into one report, noting any relevant differences in the appropriate sections.

This was our first audit of the security controls surrounding BENEFEDS and FLTCIP. We discussed the results of our audit with OPM and LTCP representatives at an exit conference.

Objectives

Our objective was to perform an evaluation of the systems' security controls to ensure that OPM and LTCP 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 BENEFEDS and FLTCIP, 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 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 the BENEFEDS and FLTCIP systems, including IT security controls in place as of June 2014.

We considered the systems' 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 LTCP and individuals at OPM with BENEFEDS and FLTCIP 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 BENEFEDS and FLTCIP 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 systems' 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. This audit was conducted from January 2014 through March 2014 in OPM's Washington, D.C. office. This was our first audit of the security controls surrounding BENEFEDS and FLTCIP.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether HI and LTCP's management of BENEFEDS and FLCIP is consistent with applicable standards. Nothing came to our attention during this review to indicate that HI and LTCP are in violation of relevant laws and regulations.

Results

I. Security Assessment and Authorization

The Security Assessment and Authorizations (SA&As) of BENEFEDS and FLTCIP were completed in March 2013.

OPM's Chief Information Security Officer reviewed the SA&A packages and signed both systems' authorization letters on March 1, 2013. The systems' authorizing official signed the letters and authorized the continued operation for the systems on March 4, 2013.

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. Both SA&As appear 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.

These documents provide guidance for analyzing information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. Both the BENEFEDS and FLTCIP systems are categorized as a moderate impact level for confidentiality, integrity, and availability, resulting in an overall categorization of "moderate."

The security categorization of both systems 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[1], 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.

[1] Revision 4 to NIST SP 800-53 was released in April 2013. OPM allows systems one year to implement the controls for the new revision. NIST SP 800-53 controls testing took place in March 2014 for this audit; therefore Revision 3 was used as criteria.

The SSPs for BENEFEDS and FLTCIP were created using the template outlined in NIST SP 800-18 Revision 1. We reviewed the BENEFEDS and FLTCIP SSPs and determined they adequately address each of the elements suggested by NIST.

IV. Security Assessment Plan and Report

Security Assessment Plans (SAP) were completed for BENEFEDS and FLTCIP in July 2012 as a part of the systems' SA&A process. Security Assessment Reports (SAR) were also completed for each system in February 2013. The SAPs and SARs were conducted by a contractor that was operating independently from HI and LTCP. We reviewed these 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.

The SAPs outlined the assessment approach for each system. The SAR for BENEFEDS identified 14 total weaknesses that were discovered as a result of the assessment; 12 of those weaknesses have since been remediated. The SAR for FLTCIP identified 7 total weaknesses, 5 of which have since been remediated. All weaknesses were added to the BENEFEDS and FLTCIP combined Plan of Action & Milestones (POA&M) document. A risk rating was applied to each weakness to determine the potential impact of exploitation.

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

V. Security Control Self-Assessment

OPM requires that the IT security controls of each contractor-operated application be tested on an annual basis. In the years that an independent assessment is not being conducted on a system as part of an SA&A, the system's owner must ensure that annual controls testing is performed by a government employee or an independent third party.

LTCP provided us with evidence that a security controls test was conducted in 2013 by an independent third-party. The assessment included a review of some relevant security controls outlined in NIST SP 800-53 Revision 3. However, the tests results were not submitted to the OCIO on the standard template. Furthermore, the documentation provided did not clearly identify which NIST controls were tested. Although it is evident that some security control test work was conducted, we are unable to verify that one-third of the NIST SP 800-53 Revision 3 controls were adequately tested, as required by OPM policy.

Recommendation 1

We recommend that HI ensure that annual security control testing is conducted in accordance with OPM policy and that the test results are submitted using the template created by the OCIO.

HI Response:

"The management of the BENEFEDS/FLTCIP systems concurs with each of the recommendations in the Draft audit and has identified a corrective action plan to address those audit findings determined to be unresolved as of the date of the OIG report."

OIG Reply:

As part of the audit resolution process, we recommend that the HI provide Internal Oversight and Compliance with evidence that it has adequately implemented this recommendation. This statement also applies to all subsequent recommendations, as the HI response above addresses all of the recommendations in the audit report.

VI. Contingency Planning and Contingency Plan Testing

NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems and Organizations, 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 BENEFEDS and FLTCIP contingency plans document the functions, operations, and resources necessary to restore and resume system operations when unexpected events or disasters occur. Both contingency plans closely follow the format suggested by NIST SP 800-34 Revision 1, and contain a majority of the required 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 tabletop and failover test was conducted for the BENEFEDS and FLTCIP systems by LTCP officials in August 2013. The exercise tested the communication and coordination between the LTCP staff and the contracted backup site personnel. The testing documentation contained an analysis and review of the results. We reviewed the testing documentation and determined that the tests conformed to NIST 800-34 Revision 1 guidelines.

VII. 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.

LTCP completed a Privacy Threshold Analysis of the BENEFEDS and FLTCIP systems and determined that a PIA was required. PIAs were completed for both systems in February 2013 and approved by the system owner and Chief Information Officer.

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 BENEFEDS and FLTCIP POA&Ms and verified that they follow the format of OPM's standard template and have 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 the POA&Ms for those systems.

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 BENEFEDS and FLTCIP. We tested approximately 62 security controls outlined in NIST SP 800-53 Revision 3. 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 BENEFEDS and FLTCIP 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, with the following exceptions:

1. Control AC-5 – Separation of Duties

LTCP does not maintain a documented policy or security matrix to outline the required segregation of duties related to the user roles in the BENEFEDS and FLTCIP systems.

NIST SP 800-53 Revision 3 states that organizations should separate duties of individuals as necessary, to prevent malevolent activity without collusion, document separation of duties, and implement separation of duties through assigned information system access authorizations. Failure to ensure separation of duties increases the risk that the application users could make unauthorized or malicious changes to the application.

Recommendation 2

We recommend that HI ensure that a policy is developed to establish proper segregation of duties within BENEFEDS and FLTCIP.

Recommendation 3

We recommend that HI ensure that a routine audit of user accounts is conducted to verify compliance with the segregation of duties policy.

2. Control CM-2 Baseline Configuration

LTCP has not documented baseline configurations for server operating systems. We were provided documentation indicating that a project is in place to establish baseline security configurations, but the process is not complete.

NIST SP 800-53 Revision 3 states that organizations should develop, document, and maintain a current baseline configuration of the information system. Failure to establish approved system configuration settings increases the risk that the systems may not meet performance and security requirements defined by the organization.

Recommendation 4

We recommend that HI ensure that LTCP documents approved security configuration settings/baselines for all operating systems used to support the BENEFEDS and FLTCIP systems.

3. Control CM-6 – Configuration Settings

LTCP does not conduct routine configuration compliance auditing. As mentioned above, LTCP does not maintain approved server configurations, and therefore cannot effectively audit security settings (i.e., there are no approved settings to which to compare the actual settings).

NIST SP 800-53 Revision 3 states that the organization should monitor and control changes to configuration settings in accordance with organizational policies and procedures. Failure to implement a thorough configuration compliance auditing program increases the risk that insecurely configured servers remain undetected, creating a potential gateway for malicious virus and hacking activity that could lead to data breaches.

Recommendation 5

We recommend that HI ensure that LTCP routinely audits the security configuration settings of its servers using approved baselines.

4. Control PE-3 – Physical Access Control

The physical access controls in LTCP's data center could be improved.

The LTCP's facility uses electronic card readers to control access to the building and data center. However, the data center did not contain general controls that we typically observe at similar facilities, including:

- Multi-factor authentication to enter the computer room (e.g., cipher lock or biometric device in addition to an access card); and

- Technical or physical control to detect or prevent piggybacking (e.g., turnstiles, piggybacking alarms, two door "man traps," etc.).

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to LTCP's data center and the sensitive resources and data it contains. NIST SP 800-53 Revision 3 provides guidance for adequately controlling physical access to information systems containing sensitive data (see control PE-3, Physical Access Control).

During the course of the audit multi-factor authentication to the computer room was implemented.

Recommendation 6

We recommend that HI ensure the improvement of the physical access controls at the FLTC data center hosting BENEFEDS and FLTCIP by installing additional controls to prevent piggybacking.

5. Control RA-5 – Vulnerability Scanning

LTCP conducts monthly vulnerability scans on its network environment. However, we conducted independent vulnerability scans on a sample of BENEFEDS and LTCIP servers, [redacted] We provided the detailed results of our scans to LTCP while on-site.

We were also told that LTCP does not have a process to document or track patch exceptions (patches that cannot be installed because they would have an adverse effect on existing systems or applications).

NIST 800-53 Revision 3 states that the organization should scan for vulnerabilities in the information system and hosted applications and remediate legitimate vulnerabilities in accordance with an organization risk assessment. Failure to remediate critical vulnerabilities increases the risk that systems could be hacked and sensitive data could be compromised.

Recommendation 7

We recommend that HI ensure that LTCP remediate the critical weaknesses identified in our vulnerability scans.

Recommendation 8

We recommend that HI ensure that LTCP document patch exceptions.

6. Control SC-7 Boundary Protection

LTCP has implemented firewalls to help secure its network environment. However, a firewall hardening policy has not been developed, and there is no routine review of the firewall configuration.

NIST SP 800-53 Revision 3 states that an organization should establish a traffic flow policy for each managed interface, document and review each exception to the traffic flow policy, and remove exceptions that are no longer supported by a business need.

Failure to implement a thorough firewall configuration policy and continuously manage the devices' settings increases the organization's exposure to insecure traffic and vulnerabilities.

Recommendation 9

We recommend that HI ensure that LTCP documents a formal firewall management policy.

Recommendation 10

We recommend that HI ensure that LTCP implement a process to conduct routine configuration reviews on its network firewalls to ensure performance and security optimization, as defined by the organizational policies.

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], Lead IT Auditor
- [redacted], Lead IT Auditor
- [redacted] IT Auditor
- [redacted], IT Auditor

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
1900 E Street, NW, Washington, DC 20415

Healthcare and
Insurance

June 30, 2014

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

FROM: [redacted]
Deputy Assistant Director, Federal Employee Insurance Operations
BENEFEDS/FLTCIP System Owner

SUBJECT: Management Response to Draft Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's BENEFEDS and Federal Long Term Care Insurance Program (FLTCIP) Systems (Report No. 4A-RI-00-14-036)

The Office of Personnel Management (OPM) Federal Employee Insurance Operations Program Office and its contractor, Long Term Care Partners, LLC; acknowledge and accept the findings of the Office of Inspector General (OIG) as documented in Report No. 4A-RI-00-14-036 for both the BENEFEDS and Federal Long Term Care Insurance Program (FLTCIP) Systems.

The management of the BENEFEDS/FLTCIP systems concurs with each of the recommendations in the Draft audit and has identified a corrective action plan to address those audit findings determined to be unresolved as of the date of the OIG report. The plan elements are provided in the attached spreadsheet. The process to identify required resources, identify milestones, respond to the risk (acceptance, transfer, mitigation/remediation), complete planned work, and provide evidence of mitigation/remediation will follow the OPM standard operating procedure for Plan of Actions and Milestones (POA&M) management. Those recommendations outlined in the report that cannot or should not be implemented due to technical limitations, significant negative impacts to performance or service delivery, or other factors will be communicated to OPM Internal Oversight and Compliance and the OPM IT Security and Privacy (ITSP) Office for review and discussion prior to any risk acceptance decision.

If you have questions about implementation of the POA&M's, please contact [redacted] Designated Security Officer, and [redacted].