U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S FEDERAL FINANCIAL SYSTEM

Report Number 4A-CF-00-19-027
October 8, 2019

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Federal Financial System

Report No. 4A-CF-00-19-027 **October 8, 2019**

Why Did We Conduct The Audit?

The Federal Financial System (FFS) is part of the Benefits Financial Management System (BFMS). BFMS is one of the U.S. Office of Personnel Management's (OPM) major information technology (IT) systems. The Digital Accountability and Transparency Act of 2014 and the Federal Information Security Modernization Act requires that the Office of the Inspector General perform audits of IT security controls of agency systems.

What Did We Audit?

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

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls of FFS and its host system, BFMS, determined that:

- A Security Assessment and Authorization (Authorization) of BFMS was completed in 2016. An Authorization was granted for up to three years.
- The security categorization of BFMS is consistent with Federal Information Processing Standards 199 and NIST Special Publication (SP) 800-60, and we agree with the "moderate" categorization.
- OPM has not fully completed a Privacy Threshold Analysis and Privacy Impact Assessment for BFMS.
- The BFMS System Security Plan follows the Office of the Chief Information Officer template, and is complete and up to date.
- The BFMS risk assessment included all known control weaknesses.
- Continuous Monitoring for BFMS was conducted in accordance with the agency's quarterly schedule for fiscal year 2019.
- A contingency plan was developed for BFMS, is in compliance with NIST SP 800-34, Revision 1, and Office of the Chief Information Officer guidance, and was tested in 2018.
- The BFMS Plan of Action and Milestones documentation included all required information and known weaknesses. However, most remediation activities are past their scheduled completion dates.
- We evaluated a subset of the system controls outlined in NIST SP 800-53, Revision 4. We determined most of the security controls tested appear to be in compliance; however, we did note one area for improvement regarding vulnerability scanning.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
BFMS	**Benefits Financial Management System**
DATA Act	**Digital Accountability and Transparency Act**
FFS	**Federal Financial System**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
OCFO	**Office of the Chief Financial Officer**
OCIO	**Office of the Chief Information Officer**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
POA&M	**Plan of Action and Milestones**
SP	**Special Publication**
SSP	**System Security Plan**

TABLE OF CONTENTS

I. BACKGROUND

The 2002 Federal Information Security Management Act requires: (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the U.S. Office of Management and Budget (OMB) on the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. The 2014 Federal Information Security Modernization Act (FISMA) reaffirmed the objectives of the prior Act.

The 2014 Digital Accountability and Transparency Act of 2014 (DATA Act) requires the Office of the Inspector General (OIG) to: (1) review a statistically valid sampling of the spending data submitted under the DATA Act by the Federal agency; and (2) submit to Congress and make publically available a report assessing the completeness, timeliness, quality, and accuracy of the data sampled and the implementation and use of data standards by the Federal agency. In accordance with the DATA Act, we conducted an evaluation of the U.S. Office of Personnel Management's (OPM) systems, processes, and internal controls in place over financial data management.

The Federal Financial System (FFS) is a commercial-off-the-shelf general ledger application used to record financial transactions for OPM. The FFS application is a part of OPM's Benefits Financial Management System (BFMS), one of the agency's major information technology (IT) systems. BFMS is comprised of several applications used by OPM's Office of the Chief Financial Officer's (OCFO) Trust Fund Group to track and report on financial accounts and transactions. Many of the security controls for FFS are inherited from BFMS or the agency's Enterprise Server Infrastructure (i.e., mainframe) and Local Area Network / Wide Area Network General Support Systems. Not only is FFS a part of a major IT system on OPM's FISMA inventory, FFS is also one of the key systems that provides data for reports required by the DATA Act.

This was our fourth audit of the IT security controls for FFS. The previous audits resulted in findings and recommendations documented in Report No. 4A-CF-00-04-077, dated September 28, 2004; Report No. 4A-CF-00-10-018 dated September 10, 2010; and Report No. 4A-CF-00-17-044, dated September 29, 2017. Six of the nine recommendations from the most recent audit have been closed. The three open recommendations are discussed below in the "Audit Findings and Recommendation" section.

OPM's Office of the Chief Information Officer (OCIO) and OCFO share responsibility for implementing and managing the IT security controls of FFS. We discussed the results of our audit with the OCIO and the OCFO representatives at an exit conference.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Our objective was to perform an evaluation of the security controls for FFS to ensure that the OCIO and the OCFO officials have managed the implementation of IT security policies and procedures in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual, and OPM's OCIO.

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

- Security Assessment and Authorization;
- Federal Information Processing Standards Publication (FIPS) Analysis;
- Privacy Impact Assessment;
- System Security Plan;
- Security Assessment Plan and Report;
- Continuous Monitoring;
- Contingency Planning and Contingency Plan Testing;
- Plan of Action and Milestones Process; and
- NIST Special Publication (SP) 800-53, Revision 4, Security Controls.

SCOPE AND METHODOLOGY

We conducted this performance audit in accordance with the Generally Accepted Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures that we considered necessary. The audit covered security controls and FISMA compliance efforts of OPM officials responsible for the FFS, including the evaluation of IT security controls in place as of July 2019.

We considered the FFS internal control structure in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objective.

To accomplish our objective, we interviewed representatives of OPM's OCIO and OCFO program offices with FFS security responsibilities, reviewed documentation and system screenshots and viewed demonstrations of system capabilities. We also reviewed relevant OPM IT policies and procedures, federal laws, OMB policies and guidance, and NIST guidance. As appropriate, we conducted compliance tests to determine the extent to which established controls and procedures are functioning as required.

Details of the security controls protecting the confidentiality, integrity, and availability of the FFS are located in the "Audit Findings and Recommendations" section of this report. Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the FFS internal controls taken as a whole. The criteria used in conducting this audit include:

- OPM Information Security Privacy and Policy Handbook;
- OPM Security Assessment and Authorization Guide;
- OMB Circular A-130, Appendix I, Responsibilities for Protecting and Managing Federal Information Resources;
- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- The Federal Information System Controls Audit Manual;
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems;

- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;

- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;

- NIST SP 800-60, Revision 1, Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories; and

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

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

The OPM Office of the Inspector General, as established by the Inspector General Act of 1978, as amended, performed the audit. We conducted the audit from April 2019 through July 2019 at OPM's Washington, D.C. office.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether OPM's management of the FFS is consistent with applicable standards. While generally compliant, with respect to the items tested, OPM was not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATION

A. SECURITY ASSESSMENT AND AUTHORIZATION

Security Assessment and Authorization (Authorization) includes: 1) a comprehensive assessment that attests that a system's security controls are meeting the security requirements of that system and 2) an official management decision to authorize operation of an information system and accept its known risks. OMB's Circular A-130, Appendix I, mandates that all Federal information systems have a valid Authorization. Although OMB previously required periodic Authorizations every three years, Federal agencies now have the option of continuously monitoring their systems to fulfill the Authorization requirement. However, as OPM does not yet have a mature program in place to continuously monitor system security controls, an Authorization is required for all OPM systems at least once every three years, as required by OPM policy.

BFMS most recently received an Authorization on November 16, 2016. This Authorization is good for up to three years and includes provisions that the system owner monitor and remediate identified weaknesses on an ongoing basis.

B. FIPS 199 ANALYSIS

The E-Government Act of 2002 requires Federal agencies to categorize all Federal information and information systems. FIPS 199 provides guidance on how to assign appropriate categorization levels for information security according to a range of risk levels.

NIST SP 800-60, Revision 1, Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories, provides an overview of the security objectives and impact levels identified in FIPS 199.

The BFMS security categorization documentation analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. BFMS is categorized with a "moderate" impact level for each of these areas, resulting in an overall categorization of "moderate."

The security categorization of BFMS appears to be consistent with FIPS Publication 199 and NIST SP 800-60 requirements, and we agree with the categorization of moderate.

C. PRIVACY IMPACT ASSESSMENT

The E-Government Act of 2002 requires agencies to perform a Privacy Threshold Analysis of Federal information systems to determine if a Privacy Impact Assessment is required for that system. OMB Memorandum M-03-22 outlines the necessary components of a Privacy Impact Assessment. The purpose of the assessment is to evaluate and document any personally identifiable information maintained by an information system.

A Privacy Threshold Analysis and Privacy Impact Assessment were partially performed on BFMS (to include FFS) in September 2016. However, both documents are incomplete (e.g., required questions were left unanswered) and neither has been formally approved and signed.

This finding is consistent with the open recommendation in the fiscal year 2017 FFS audit report (Report No. 4A-CF-00-17-044, Recommendation 1) that recommends OPM fully complete and approve a Privacy Impact Assessment for BFMS.

D. SYSTEM SECURITY PLAN

Federal agencies must implement, for each information system, the security controls outlined in NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in a System Security Plan (SSP) for each system, and provides guidance for doing so.

The SSP for BFMS was created using the OCIO's SSP template that utilizes NIST SP 800-18, Revision 1, as guidance. The template requires that the SSP contain the following elements:

- System Name and Identifier;
- System Owner;
- Authorizing Official;
- Other Designated Contacts;
- Assignment of Security Responsibility;
- System Operational Status;
- General Description/Purpose;
- Information System Type;
- System Environment;
- System Interconnection/Information Sharing;

- System Categorization;
- Security Control Selection;
- Completion and Approval Dates.
- Minimum Security Controls;
- Laws, Regulations, and Policies Affecting the System; and

The current BMFS SSP was last updated in March 2019. We reviewed the BFMS SSP and determined that it is up to date, accurate, and has been signed by the system owner.

Nothing came to our attention to indicate that the BFMS SSP was inadequate.

E. SECURITY ASSESSMENT PLAN AND REPORT

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

The BFMS Security Assessment Plan and Security Assessment Report were completed by OPM IT security staff in August 2016 and April 2019, respectively, as a part of the system's Authorization process. 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.

The Security Assessment Report was updated to include all 30 of the weaknesses identified in the assessment results table. The risk assessment table also includes all identified weaknesses.

Nothing came to our attention to indicate that the BFMS Security Assessment Plan and Security Assessment Report were inadequate.

F. CONTINUOUS MONITORING

OPM requires that the IT security controls of each system be assessed on a continuous basis. OPM's OCIO has developed an Information Security Continuous Monitoring Plan that includes a template outlining the security controls that must be tested for all information systems. All system owners are required to tailor the Information Security Continuous Monitoring Plan template to each individual system's specific security control needs and then test the system's

security controls on an ongoing basis. The test results must be provided to the OCIO on a routine basis for centralized tracking.

We reviewed the BFMS Information Security Continuous Monitoring submissions from the first and second quarter of fiscal year 2019. The BFMS Information Security Continuous Monitoring submissions follow the required template, contain properly documented test methods and results, and the testing schedule is in accordance with the OPM Information Security Continuous Monitoring Plan.

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

G. CONTINGENCY PLANNING AND CONTINGENCY PLAN TESTING

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

1. Contingency Plan

The BFMS contingency plan was updated in October 2018 and documents the functions, operations, and resources necessary to restore and resume BFMS when unexpected events or disasters occur. The contingency plan adequately follows the format suggested by NIST SP 800-34, Revision 1, and OPM's template for contingency plans.

Nothing came to our attention indicating that the BFMS contingency plan was inadequate.

2. Contingency Plan Testing

Contingency plan testing is a critical element of a viable disaster recovery capability. OPM requires that contingency plans be tested annually to determine the plan's effectiveness and the organization's readiness to execute the plan. NIST SP 800-34, Revision 1, provides guidance for testing contingency plans and documenting the results.

The most recent contingency plan test for FFS was conducted in May 2018.

Nothing came to our attention indicating that the BFMS contingency plan testing process was inadequate.

H. PLAN OF ACTION AND MILESTONES PROCESS

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

BFMS has a total of 30 open POA&M entries and 20 are past the scheduled completion dates.

In 2017, BFMS had a total of 46 open POA&M entries. Of those, 45 were past the scheduled completion dates. Currently, BFMS has a total of 30 open POA&M entries and 20 are past the scheduled completion dates. While we understand that POA&Ms can be delayed due to resource constraints, it is imperative that POA&M documentation be updated so that the current risks to the system can be understood. The POA&M process is used to track both the progress and the delays in the remediation of system weaknesses so that resources may be efficiently used when available.

This finding is consistent with the open recommendation in the fiscal year 2017 FFS audit report (Report No. 4A-CF-00-17-044, Recommendation 7) that recommends OPM develop a detailed action plan to remediate all overdue POA&M items. This action plan should include realistic estimated completion dates.

I. NIST SP 800-53 EVALUATION

NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, provides guidance for implementing a variety of security controls for information systems supporting the federal government. As part of this audit, we evaluated whether a subset of these controls had been implemented for FFS and BFMS. We tested approximately 40 controls as outlined in NIST SP 800-53, Revision 4, including one or more controls from each of the following control families:

- Access Control;
- Audit and Accountability;
- Configuration Management;
- Contingency Planning;

- Identity and Authentication;
- Planning;
- Risk Assessment;
- Security Assessment and Authorization; and
- System and Information Integrity.

These controls were evaluated by interviewing individuals with system security responsibilities, reviewing documentation and system screenshots, viewing demonstrations of system capabilities, and conducting tests directly on the system. We determined that the majority of the tested security controls appear to be in compliance with NIST SP 800-53, Revision 4, requirements, with the exceptions detailed below.

1. Control RA-5 – Vulnerability Scanning of Mainframe

OPM does not currently conduct vulnerability scans of the mainframe.

OPM does not currently possess the tools necessary to conduct vulnerability scans of the mainframe. To address this security weakness, OPM submitted a Request for Information regarding the acquisition of IBM's Z/Assure, a mainframe vulnerability assessment tool, and is awaiting industry response.

NIST SP 800-53, Revision 4, requires that "The organization … scans for vulnerabilities in the information system and hosted applications … ."

Failure to scan the mainframe can leave the system vulnerable to security breaches.

Recommendation 1

We recommend that OPM conduct an analysis to determine the viability of acquiring a vulnerability scanning tool for the mainframe.

Note: In the event the decision is made not to acquire a tool and implement vulnerability scanning of the mainframe environment, we recommend that OPM conduct a risk assessment and the BFMS Authorizing Official formally accepts the risks.

OPM Response:

"We concur and are performing market research for procurement in [FY 2020], subject to the availability of funds."

OIG Comment:

As part of the audit resolution process, we recommend that the OCIO provide OPM's Internal Oversight and Compliance office with evidence that this recommendation has been implemented.

2. Control SI-2 – Flaw Remediation

In 2017, we identified that OPM did not have a support contract in place for FFS since 2002.

This finding led to an open recommendation in the fiscal year 2017 FFS audit report (Report No. 4A-CF-00-17-044, Recommendation 9) that recommends OPM develop and implement a plan to replace FFS with a fully supported financial system.

As a part of this audit, we reviewed documents for a long-term plan that were sufficient to satisfy this recommendation. Therefore, we support closure of this prior recommendation. While the development of a plan to replace FFS does not address the weakness inherent in the finding, (i.e., that FFS is not currently supported by the vendor), we do feel that OPM has acknowledged the risks and is taking the correct steps to address this weakness. We will continue to monitor OPM's progress to execute the larger modernization plan as it applies to replacing the system functionality and decommissioning FFS. We will follow up on this issue in our 2021 DATA Act compliance audit.

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Chief Information
Officer

SEP 0 5 2019

MEMORANDUM FOR: [redacted]
CHIEF, INFORMATION SYSTEMS AUDIT GROUP
OFFICE OF INSPECTOR GENERAL

FROM: CLARE A. MARTORANA
Chief Information Officer

DENNIS COLEMAN
Chief Financial Officer

SUBJECT: Management Response to OIG Audit of the Information Technology Security Controls of OPM's Federal Financial System Compliance with FISMA and Data Act
(Report Number 4A-CF-00-19-027)

Thank you for providing OPM the opportunity to respond to the Office of the Inspector General (OIG) draft report, Audit of the Information Technology Security Controls of OP M's Federal Financial System Compliance with FISMA and Data Act, Report Number 4A-CF-00-19-027, dated August 15, 2019.

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

Recommendation 1: We recommend that OPM conduct an analysis to determine the viability of acquiring a vulnerability scanning tool for the mainframe.

Note: In the event the decision is made not to acquire a tool and implement vulnerability scanning of the mainframe environment, we recommend that OPM conduct a risk assessment and the BFMS Authorizing Official formally accepts the risks.

Management Response: We concur and are performing market research for procurement in FY20, subject to the availability of funds.

We appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact [redacted] at [redacted]@opm.gov.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone:

Toll Free Number:	(877) 499-7295
Washington Metro Area:	(202) 606-2423

By Mail:

Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100