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 Benefits Financial Management System

Report Number 4A-CF-00-21-010
September 14, 2021

Executive Summary

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

Report No. 4A-CF-00-21-010 **September 14, 2021**

Why Did We Conduct the Audit?

The Benefits Financial Management System (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 (FISMA) requires that the Office of the Inspector General perform audits of IT security controls of agency systems.

What Did We Audit?

We completed a performance audit of BFMS to ensure that the system's security controls meet the standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual, and OPM's Office of the Chief Information Officer (OCIO).

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls of the BFMS determined that:

- A Security Assessment and Authorization Authorization) was completed in December 2020. The Authorization was granted for up to 18 months.
- The BFMS security categorization is consistent with Federal Information Processing Standards 199 and we agree with the "moderate" categorization.
- OPM does not have an approved Privacy Impact Assessment for the BFMS.
- The BFMS System Security Plan was complete and follows the OCIO's template.
- The Office of the Chief Financial Officer appropriately performed a security control assessment
- Continuous Monitoring for the BFMS was conducted in accordance with the OPM's quarterly schedule for fiscal year 2020.
- The BFMS contingency plan test was not performed within the required annual cycle.
- The BFMS Plan of Action and Milestones documentation is up to date and contains all identified weaknesses.
- We evaluated a subset of the system controls outlined in NIST Special Publication 800-53, Revision 4. We determined all of the security controls tested appear to be in compliance.

Abbreviations

Authorization	**Security Assessment and Authorization**
BFMS	**Benefits Financial Management System**
DATA Act	**Digital Accountability and Transparency Act of 2014**
FFS	**Federal Financial System**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology's Special Publication**
OCFO	**Office of the Chief Financial Officer**
OCIO	**Office of the Chief Information Officer**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
POA&M	**Plan of Action and Milestones**
SSP	**System Security Plan**

Table of Contents

I. Background

On December 17, 2002, the President signed into law the E-Government Act (P.L. 107 347), which includes Title III, the Federal Information Security Management Act. It requires (1) annual agency program reviews, (2) annual Inspector General evaluations, (3) agency reporting to the U.S. Office of Management and Budget (OMB) the results of Inspector General evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In 2014, Public Law 113-283, the Federal Information Security Modernization Act (FISMA) was established and reaffirmed the objectives of the prior Act.

On May 9, 2014, the President signed into law the Digital Accountability and Transparency Act of 2014 (DATA Act) (P.L. 113-101) which includes Section 6, Accountability for Federal Funding. It requires Inspector Generals to (1) review of a statistically valid sampling of the spending data submitted under the DATA Act by the Federal agency; and (2) submit to Congress and make publicly 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 are conducting an evaluation of the U.S. Office of Personnel Management (OPM)'s 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. The 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 the FFS are inherited from the BFMS or the agency's Enterprise Server Infrastructure (i.e., mainframe) and Local Area Network / Wide Area Network General Support Systems. Not only is the FFS a part of a major IT system on OPM's FISMA inventory, the FFS is also one of the key systems that provides data for reports required by the DATA Act.

This was our fifth audit of the IT security controls for the BFMS. 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; Report No. 4A-CF-00-17-044, dated September 29, 2017; and Report No. 4A-CF-00-19-027, dated October 8, 2019. Two of the three recommendations from the most recent audit have been closed. The open recommendation is discussed below in the "Audit Findings and Recommendation" section, along with a new recommendation identified in this audit.

OPM's Office of the Chief Information Officer (OCIO) and OCFO share responsibility for implementing and managing the IT security controls of the BFMS. 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 audit of the security controls for the BFMS to ensure that the OCIO 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, 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 BFMS, including:

- Security Assessment and Authorization;
- Federal Information Processing Standards Publication 199 (FIPS 199) 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 (POA&M) 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 BFMS, including the evaluation of IT security controls in place as of May 2021.

We considered the BFMS 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 with security responsibilities for BFMS, reviewed documentation and system screenshots, viewed demonstrations of system capabilities, and conducted tests directly on the system. 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.

In conducting our audit, we relied to varying degrees on computer-generated data provided by OPM. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps, but we determined that it was adequate to achieve our audit objectives. However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.

As part of this audit, we tested a judgmental sample of NIST SP 800-53, Revision 4, controls. We chose a sample of 76 controls from a universe of 263 "moderate" controls. The sample included at least one control from each NIST control family. The judgmental sample was drawn from applicable controls that were identified in the latest security control assessment as "in place" and "system-specific." The results of the judgmentally selected sample were not projected to the population since it is unlikely that the results are representative of the population.

Our assessment of the security controls protecting the confidentiality, integrity, and availability of the BFMS is in the "Audit Findings and Recommendation" 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 BFMS internal controls taken as a whole. The criteria used in conducting this audit included:

- OPM Security Assessment and Authorization Guide;
- OPM Contingency Planning Policy;
- OPM Security Authorization Policy;
- 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; and
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether OPM's management of the BFMS 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

A 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, OPM does not yet have a mature program in place to continuously monitor system security controls, therefore an Authorization is required for all OPM systems at least once every three years as required by OPM policy.

The BFMS was authorized to operate in December 2020. The Authorization is valid for up to 18 months and includes provisions that the system owner monitor and remediate identified weaknesses on an ongoing basis.

The BFMS Authorization is valid for up to 18 months after December 2020.

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

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 area – confidentiality, integrity, and availability – resulting in an overall categorization of "moderate."

The security categorization of the BFMS appears to be consistent with FIPS 199 and NIST SP 800-60, Revision 1, requirements, and we agree with the categorization of "moderate."

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

C. Privacy Impact Assessment

The E-Government Act of 2002 requires agencies to perform a Privacy Threshold Analysis (PTA) of Federal information systems to determine if a Privacy Impact Assessment (PIA) is required for that system. In accordance with OPM policies requiring annual review and approval, the BFMS Privacy Threshold Analysis was drafted by OPM in 2014. The PTA was incomplete and was not signed by the Chief Privacy Officer. However, OPM acknowledges that a PIA is required for the 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. Currently, there is no drafted or approved PIA for the BFMS.

The OPM Privacy Impact Assessment Guide states, "All OPM IT systems must have a PTA." According to the OPM Security Authorization policy, the Chief Privacy Officer must "Review and approve the selection of privacy controls for new information systems prior to the implementation of the privacy controls."

Incomplete and outdated PTA and PIA documents increase the risk that Personally Identifiable Information can be compromised and the likelihood that the system is not in compliance with privacy laws and regulations.

The finding is consistent with the open recommendation in the 2017 FFS audit report (Report No. 4A-CF-00-17-044, Recommendation 1) which recommends that OPM fully completes and approves a PIA for the BFMS. We continue to recommend that OPM remediate this deficiency.

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 OCFO developed the BFMS SSP using the OCIO's SSP template which uses NIST SP 800-18, Revision 1, as guidance. The template requires the SSP to 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;
- Laws, Regulations, and Policies Affecting the System;
- Security Control Selection;
- Minimum Security Controls; and
- Completion and Approval Dates.

We reviewed the current BFMS SSP, last updated in June 2020, and determined that it adequately reflects the system's current state. Nothing came to our attention to indicate that the BFMS system security plan has not been properly documented and approved.

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. A Risk Assessment Report assesses the risk to the system for each weakness identified during the security controls assessment.

The BFMS Security Assessment Plan and Risk Assessment Report were created by the OCIO Information System Security Officer in July 2020 and September 2020, respectively. 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.

All applicable controls were assessed by the independent assessor. All risks were assessed and POA&Ms were created for all controls that were not mitigated or resolved. Nothing came to our attention to indicate that the BFMS Security Assessment Plan or Risk 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.

A review of the continuous monitoring submissions revealed that over 160 distinct controls were tested.

We received the fiscal year 2020 quarterly continuous monitoring submissions for BFMS. A review of the submissions revealed that over 160 distinct controls were tested.

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, updated in June 2020, documents the functions, operations, and resources necessary to restore and resume the BFMS when unexpected events or disasters occur. The contingency plan follows the format suggested by NIST SP 800-34, Revision 1, and OPM's template for contingency plans.

We did not detect any issues with the BFMS contingency plan.

2) Contingency Plan Testing

Contingency plan testing is a critical element of a viable disaster recovery capability. OPM requires that contingency plans for all systems be tested annually to evaluate 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 OCFO updated the BFMS contingency plan during the 2020 fiscal year. However, the OCFO did not perform a contingency plan test for the system. The most recent contingency plan test was performed in August 2019.

NIST SP 800-53, Revision 4 states that the organization, "Tests the contingency plan for the information system [organization-defined frequency] using [organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan." OPM's Contingency Planning Policy requires system owners to perform annual tests of the contingency plan.

Failure to test a contingency plan increases the risk that OPM will not be effective in recovering systems in the event of an unplanned outage.

Recommendation 1

We recommend that the OCFO perform a functional contingency plan test on the BFMS in accordance with OPM's Contingency Planning Policy.

OPM Response:

"We concur. OPM plans to conduct a Disaster Recovery (DR) exercise, which will include the functional contingency plan test on BFMS, in accordance with OPM's Contingency Planning Policy during the 2021 fiscal year. Once the DR exercise is completed and the closure package approved, OPM will provide closure evidence to the OIG."

OIG Response:

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.

H. Plan of Action and Milestones

A 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.

The BFMS has 13 active POA&M weaknesses, with 1 in an initial status. The POA&M that is in initial status was identified in the fourth quarter of fiscal year 2020. OPM's POA&M guide does not define a timeliness requirement to move a POA&M from initial to open status, but this deficiency was addressed in Report No. 4A-CI-00-20-009 Recommendation 11. The other BFMS POA&Ms are properly formatted according to OPM policy and all weaknesses are properly documented, to include attainable closure dates.

BFMS has 13 active POA&M weaknesses, including 1 in initial status that was identified in the fourth quarter of fiscal year 2020.

We did not detect any issues with the BFMS POA&M.

I. NIST 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 OPM has implemented a subset of these controls for the 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;
- Awareness and Training;
- Configuration Management;
- Contingency Planning;
- Identity and Authentication;
- Incident Response;
- Media Protection;
- Planning;
- Risk Assessment;
- Security Assessment and Authorization;
- System and Communications Protection;
- System and Information Integrity; and
- System and Services Acquisition.

The 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 all of the tested security controls appear to be in compliance with NIST SP 800-53, Revision 4, requirements. We did not identify any inadequacies in testing the BFMS's NIST control requirements.

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Financial Officer

June 24, 2021

Memorandum for Chief, Information Systems Audits Group
Eric W. Keehan

From: Margaret P. Pearson
Acting Chief Financial Officer

Guy V. Cavallo
Acting Chief Information Officer

Subject: Office of Personnel Management Response to the Office of the Inspector General Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Benefits Financial Management System (Report number 4A-CF-00-21-010)

Thank you for providing the Office of Personnel Management (OPM the opportunity to respondto the Office of the Inspector General (OIG) draft report, *Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Benefits Financial Management System*, Report number 4A-CF-00- 21-010, dated June 4, 2021.

Response to your recommendation including planned corrective actions, as appropriate, is provided below.

Recommendation 1: We recommend that OCFO performs a functional contingency plan test on BFMS in accordance with OPM's Contingency Planning Policy.

Management Response: We concur. OPM plans to conduct a Disaster Recovery (DR) exercise, which will include the functional contingency plan test on BFMS, in accordance with OPM's Contingency Planning Policy during the 2021 fiscal year. Once the DR

exercise is completed and the closure package approved, OPM will provide closure evidence to the OIG.

We appreciate the opportunity to respond to this draft report. If you have any questions regardingour response, please contact Darrin McConnell at (202) 606-6210, Darrin.McConnell@opm.gov.

Cc:
Janet Barnes
Rochelle Bayard
Erick Borda
Cord Chase
Darrin McConnell

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