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-00-17-044
September 29, 2017

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-00-17-044 **September 29, 2017**

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 (FISMA) require that the Office of the Inspector General (OIG) perform an audit of IT security controls of this system.

What Did We Audit?

The OIG has completed a performance audit of FFS 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 Security 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 FFS and its host system, BFMS, determined that:

- A Security Assessment and Authorization (Authorization) of BFMS was completed in 2016. An authorization to operate was granted for up to three years.
- The security categorization of BMFS is consistent with Federal Information Processing Standards 199 and NIST Special Publication (SP) 800-60, and we agree with the categorization of "moderate."
- OPM has not fully completed a Privacy Impact Assessment for BFMS.
- The BFMS System Security Plan generally follows the OCIO template, but there were instances where the documentation was incomplete or out of date.
- The CBIS risk assessment did not include an assessment of all known control weaknesses.
- OPM could improve the continuous monitoring of the security controls of BFMS.
- A contingency plan was developed for BFMS and is generally in compliance with NIST SP 800-34 Revision 1 and OCIO guidance. However, the plan is missing several pieces of critical information.
- The BFMS Plan of Action and Milestones (POA&M) documentation did not include all required information and known weaknesses. In addition, most POA&M remediation activities are more than six months past their scheduled completion dates.
- We evaluated a subset of the system controls outlined in NIST SP 800-53 Revision 4. We determined that most of the security controls tested appear to be in compliance, however, we did note two areas for improvement.

ABBREVIATIONS

ATO	**Authorization to Operate**
BFMS	**Benefits Financial Management System**
DATA Act	**Digital Accountability and Transparency Act**
FFS	**Federal Financial System**
FIPS	**Federal Information Processing Standards**
FISCAM	**Federal Information System Controls Audit Manual**
FISMA	**Federal Information Security Management Act**
IG	**Inspector General**
ISCMP	**Information Security Continuous Monitoring Plan**
IT	**Information Technology**
MRB	**Management Review Board**
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**
PIA	**Privacy Impact Analysis**
POA&M	**Plan of Action and Milestones**
PTA	**Privacy Threshold Analysis**
Authorization	**Security Assessment and Authorization**
SAP	**Security Assessment Plan**
SAR	**Security Assessment Report**
SP	**Special Publication**
SSP	**System Security Plan**

TABLE OF CONTENTS

I. BACKGROUND

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. It 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) of the results of IG 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 FISMA. As part of our evaluation, we will review the Office of Personnel Management (OPM)'s FISMA compliance strategy and document the status of their compliance efforts.

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 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 are conducting an evaluation of 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 keep record of financial transactions at 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 made up 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 generating data for DATA Act reports. As such, FISMA and the DATA Act require the OIG to perform an audit of IT security controls of this system.

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 goal was to perform an evaluation of the security controls for FFS to ensure 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 (FISCAM), and OPM's OCIO.

The audit objective was carried out by reviewing the degree to which a variety of security program elements have been implemented for FFS, including:

- Security Assessment and Authorization (Authorization);
- Federal Information Processing Standards (FIPS) 199 Analysis;
- Privacy Impact Assessment (PIA);
- System Security Plan (SSP);
- 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

This performance audit was conducted 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 FFS, including the evaluation of IT security controls in place as of July 2017.

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 objectives.

To accomplish our objective, we interviewed representatives of OPM's OCIO and OCFO program offices with FFS security responsibilities, 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.

Details of the security controls protecting the confidentiality, integrity, and availability of FFS 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 FFS' internal controls taken as a whole. The criteria used in conducting this audit include:

- OPM Information Security and Privacy Policy Handbook;
- 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;
- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- 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 the Risk Management Framework to 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, 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;

- FIPS 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 the data was sufficient to achieve the audit objectives. Except as noted above, the audit was conducted in accordance with the 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 May through July 2017 in 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 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 RECOMMENDATIONS

The following sections detail the results from our audit of OPM's Federal Financial System.

A. SECURITY ASSESSMENT AND AUTHORIZATION

A Security Assessment and Authorization (Authorization) includes 1) a comprehensive assessment attesting that the system's security controls meet security requirements 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 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 fully mature program in place to continuously monitor system security controls, so a current Authorization is required for every OPM system.

BFMS was most recently authorized to operate (ATO) on November 16, 2016. This ATO is valid for up to three years and requires the system owner to monitor and remediate identified weaknesses on an ongoing basis.

FFS was appropriately subjected to the full Authorization process.

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 for how to appropriately assign the categorization levels for 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 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 is 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 Privacy Threshold Analysis (PTA) screening of federal information systems to decide if the system needs a PIA. OMB Memorandum M-03-22 outlines the necessary elements of a PIA. The purpose of the assessment is to evaluate and document any personally identifiable information kept by an information system.

A PTA and PIA were partially completed for BFMS (to include FFS) in September 2016. However, both documents are incomplete (e.g., required questions were left unanswered) and neither document has been formally approved and signed.

OPM policy requires that "Both the PTA and PIA must be reviewed by the OPM Privacy Officer who recommends approval to the Chief Privacy Officer. These activities must be completed prior to the authorization decision . . . ."

Recommendation 1

We recommend that OPM fully completes and approves a PIA for BFMS.

OPM Response:

"OPM concurs with the intent of the recommendation; … OPM has already determined that a PIA is required for the major system and is working to update the PIA."

OIG Comment:

As part of the audit resolution process, we recommend that the OCIO provide OPM's Internal Oversight and Compliance division with evidence that this recommendation has been implemented. This statement applies to all subsequent recommendations in this audit report that the OCIO agrees to implement.

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 and guides the documentation of controls in each system's SSP.

The SSP for BFMS was created using the OCIO's SSP template, which uses NIST SP 800-18, Revision 1, as guidance. The template requires the following elements be documented within the SSP:

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

The current SSP was signed on October 4, 2016. We reviewed the BFMS SSP and determined it does not adequately address all of the requirements of NIST. Specifically, we found instances of the following issues:

- System information and required control documentation were outdated, and
- Required controls were either not documented or incompletely documented.

NIST SP 800-18, Revision 1, states "it is important to periodically assess the plan, review any change in system status, functionality, design, etc., and ensure that the plan continues to reflect the correct information about the system."

The lack of current and complete system documentation increases the risks controls are not implemented and functioning as required. This increases the difficulty of assessing risks to the system and to OPM as a whole.

Outdated, missing, and incomplete information was identified in the SSP.

Recommendation 2

We recommend that OPM update the BFMS SSP in accordance with the agency's policies and NIST standards.

OPM Response:

"OPM concurs with the recommendation. The major system SSP was updated and routed for signature after the release of the draft report. OPM will provide OIG the signed SSP to address this recommendation."

E. SECURITY ASSESSMENT PLAN AND REPORT

A Security Assessment Plan (SAP) and Security Assessment Report (SAR) were completed for BFMS in August 2016 and October 2016, respectively, as a part of the system's Authorization process. The SAP and SAR were completed by OPM IT security staff. 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 the appropriate management, operational, and technical controls were tested for a system with a "moderate" security categorization.

The assessment results table showed 49 of the 69 controls tested were not fully satisfied. Of these 49 control deficiencies identified, 38 were not included in the risk assessment of the SAR. The remaining 11 controls (those that were appropriately included in the risk assessment), were all appropriately added to the BFMS POA&Ms.

All known security weaknesses were not evaluated during the risk assessment.

OPM policy requires that each weakness identified in the assessment be assessed for risk as a part of the SAR.

Failure to assess the risk associated with all identified weaknesses increases the risk that weaknesses are not properly prioritized for remediation.

Recommendation 3

We recommend that OPM perform an analysis to assess the risk of the 38 control deficiencies that were omitted from the risk assessment, and update the BFMS risk assessment and POA&Ms to include all identified weaknesses and their risk levels.

OPM Response:

"OPM concurs with the recommendation. After receipt of the draft report, OPM reviewed the 38 security controls in question. OPM is in the process of updating the risk assessment and POA&Ms, as needed."

F. CONTINUOUS MONITORING

OPM requires that the IT security controls of each application be assessed on a continuous basis. OPM's OCIO has developed an Information Security Continuous Monitoring Plan (ISCMP) which includes a template outlining the security controls to be tested for all information systems. This template must be tailored to each individual system's specific security control needs. All system owners are required to customize their system's ISCMP and then test the system's security controls on an ongoing basis. The test results must be provided to the OCIO routinely for centralized tracking.

We reviewed the BFMS ISCMP submissions from [redacted] fiscal year 2017. Although it was apparent that control testing activity was performed for this system, we noted significant issues with the testing process:

- There were five instances where the results of the controls test were not documented;
- There were numerous instances where the testing appears to be incomplete; and
- All controls with results are marked as being fully satisfied even if non-remediated weaknesses had been previously identified for certain controls.

Failure to properly continuously monitor controls increases the likelihood of unidentified risks to the system.

Recommendation 4

We recommend that OPM test the security controls of BFMS in accordance with the ISCMP testing schedule and ensure the results are properly documented.

OPM Response:

"OPM concurs with the recommendation. After receipt of the draft report, OPM completed testing the security controls of the major system and documented the results according to OPM security procedures."

G. CONTINGENCY PLANNING AND CONTINGENCY PLAN TESTING

NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems, says 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 these plans to be routinely reviewed, tested, and updated.

1) Contingency Plan

The BFMS contingency plan 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. However, not all portions of the BFMS contingency plan have been completed. There are multiple sections of the contingency plan and 5 of its 13 appendices that do not contain all of the required information.

Failure to fully document the required contingency plan information increases the risk that adverse effects from a disruptive event cannot be mitigated.

Recommendation 5

We recommend that OPM update the BFMS contingency plan to include all required information from OPM's template.

OPM Response:

"OPM concurs with the recommendation. OPM is in the process of updating the major system contingency plan."

2) Contingency Plan Testing

Contingency plan testing is a critical element of a viable disaster recovery capability. OPM requires contingency plans to be tested routinely 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 August 2016. The test was identified as a functional test, and was marked as successful.

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

H. 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 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.

1) Incomplete POA&M Lists

We evaluated the BFMS POA&M documentation included in the Authorization package and a separate list of POA&Ms maintained by OPM in its tracking tool. Neither list was complete; the Authorization list did not include weaknesses previously identified and maintained in the tracking tool, nor was the tracking tool updated to include the weaknesses identified in the Authorization.

OPM policy requires "For systems going through a reauthorization, the POA&M also includes all other open and draft weaknesses that are on the existing POA&M as well." Without a complete list of known weaknesses, OPM is most likely underreporting the number of POA&Ms. Of greater concern, the authorizing official does not have a complete understanding of the current system risk when authorizing the system to operate.

Furthermore, the POA&Ms in the Authorization package do not adhere to OPM's POA&M template or include all of the required information (e.g., resources required for remediation, actual completion dates, milestone changes, and source information for weaknesses.)

Without complete documentation there is an increased risk weaknesses are not resolved appropriately and timely.

Recommendation 6

We recommend that OPM update the BFMS POA&M to include all identified weaknesses and required information per OPM policy.

OPM Response:

'OPM concurs with the recommendation. OPM is in transition from one POA&M tracking tool to another. After receipt of the draft report, OPM added the POA&Ms to the new tracking tool. The POA&Ms are now in the process of being updated with the required information."

2) Overdue POA&Ms

BFMS has a total of 46 open POA&M entries, and 45 have scheduled completion dates over six months overdue. Of these, 11 are more than two years overdue and 1 dates back to 2012. While we understand POA&Ms can be delayed due to resources constraints, it is imperative POA&M documentation be updated so 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 resources may be efficiently used when available.

OPM's POA&M policy states that "Should expected completion dates for milestones of POA&Ms be missed, the associated POA&Ms will be brought before the [Management Review Board (MRB)] for review in order to address any corrective actions needed for remediating the POA&Ms in accordance with the requirements defined in the [ATO] issued for the applicable system. Updated milestones and expected completion dates will be required for the following MRB meeting."

A large number of POA&Ms are significantly overdue without revised and approved remediation plans.

Failure to properly maintain a system's POA&M increases the likelihood of weaknesses not being addressed in a timely manner and potentially exposing the system to malicious attacks exploiting those unresolved vulnerabilities.

Recommendation 7

We recommend that OPM develop a detailed action plan to remediate all overdue POA&M items. This action plan should include realistic estimated completion dates.

OPM Response:

"OPM concurs with the recommendation. OPM is in the process of updating the POA&M items with new estimated completion dates, taking into consideration any factors that have led to the previously missed 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 21 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;
- System and Communications Protection; and,
- System and Information Integrity.

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

We determined the tested security controls appear to be in compliance with the requirements of NIST SP 800-53, Revision 4, with the following exceptions:

1) Control CM-6 – Configuration Settings

OPM maintains a security guide and user manual for BFMS, but these documents do not detail the approved configuration settings for the system. Configuration settings are the system options that are adjusted to enforce or enhance protection of system components and data. Documented settings are necessary so the system can be reviewed for compliance against an approved standard.

NIST SP 800-53, Revision 4, states that "Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers . . . ."

Documented configuration settings for a system ensure that security settings are configured to reduce the risk of unapproved changes.

Recommendation 8

We recommend that OPM document the approved security configuration settings for BFMS.

OPM Response:

"OPM concurs with the recommendation. OPM will assess the risk of this finding and create an action plan to apply security controls to mitigate the identified risk, where appropriate."

2) Control SI-2 – Flaw Remediation

FFS is a commercial software product developed and supported by a third-party vendor. This vendor had historically developed and released updated versions of the FFS software, but OPM has not had a support contract in place to receive these updates since 2002. Although OPM has staff in place to manage the configuration of the software (e.g., modify the system reports), this does not alleviate the operational and security risks associated with running unsupported software.

OPM has not had a support contract in place for FFS since 2002.

The Office of Management and Budget has released specific guidance that states "Agencies shall: . . . Prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement;" and details that this "includes hardware, software, or firmware components no longer supported by developers, vendors, or manufacturers through the availability of software patches, firmware updates, replacement parts, and maintenance contracts." NIST SP 800-53, Revision 4, requires that, "The organization: . . . Identifies, reports, and corrects information systems flaws . . . [and] Installs security-relevant software and firmware updates . . . ."

FISCAM states "Procedures should ensure that only current software releases are installed in information systems. [and explains the risk that] Noncurrent software may be vulnerable to malicious code such as viruses and worms."

In addition to the security risks inherent in operating an application that no longer receives updates, there are two other critical issues OPM faces by continuing to use the unsupported FFS application. First, FFS and BFMS inherit the majority of their security controls from the general support systems that host these applications (OPM's mainframe and Local Area Network / Wide Area Network). As the support systems' technology continues to evolve, the FFS application may no longer be compatible with those host environments. This could either make FFS obsolete, or it could increase the security risks of OPM as a whole should the agency refrain from updating the support systems in order to keep the FFS application operational. Second, OPM's financial reporting needs continue to evolve (e.g., new requirements from the DATA Act), and the core functionality of the FFS application cannot be updated to meet these needs. As a result, OPM must currently rely on inefficient manual processes to meet DATA Act reporting requirements.

Recommendation 9

We recommend that OPM develop and implement a plan to replace FFS with a fully supported financial system.

OPM Response:

"OPM concurs with the recommendation. OPM has embarked upon an initiative to modernize the application. As a part of this effort, OPM is in the acquisition planning stage of assessing commercially available alternatives for systems implementation services, application hosting services, operational support (post implementation including help desk

services), and Commercial Off-The-Shelf (COTS) financial management software applications. The objectives of the application replacement / Trust Funds Modernization effort are to modernize/replace the current system to facilitate greater transparency, compliance, and overall stability and sustainability of the system."

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Information Officer

August 18, 2017

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

FROM: DAVID L. DEVRIES
CHIEF INFORMATION OFFICER

DENNIS D. COLEMAN
CHIEF FINANCIAL OFFICER

Subject: Office of Personnel Management Response to the Office of the Inspector General Audit Report No. 4A-CF-00-17-044

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report 4A-CF-00-17-044. We recognize that even the most well-run programs benefit from external evaluation and we appreciate your assessment of our operations as it will help guide our improvements to enhance the security of the data provided to OPM by the Federal workforce, the Federal agencies, Private industries, and the general public.

We welcome a collaborative dialogue to help us fully understand the OIG's recommendations as we plan our remediation efforts so that our actions, and the closure of the recommendations, thoroughly address the underlying issues.

The response to your recommendations is provided below.

Recommendation 1
We recommend that OPM fully complete and approve a PTA and PIA for the [major system].

OPM Response: OPM partially concurs with the recommendation. OPM concurs with the intent of the recommendation; however, OPM has already determined that a PIA is required for the major system and is working to update the PIA. Since OPM has already created a PIA for the system, we do not intend to recreate a PTA at this time.

Recommendation 2
We recommend that OPM update the [major system] SSP in accordance with the agency's policies and NIST standards.

OPM Response: OPM concurs with the recommendation. The major system SSP was updated and routed for signature after the release of the draft report. OPM will provide OIG the signed SSP to address this recommendation.

Recommendation 3
We recommend that OPM perform an analysis to assess the risk of the 38 control deficiencies that were omitted from the risk assessment, and update the [major system] risk assessment and POA&Ms to include all identified weaknesses and their risk levels.

OPM Response: OPM concurs with the recommendation. After receipt of the draft report, OPM reviewed the 38 security controls in question. OPM is in the process of updating the risk assessment and POA&Ms, as needed.

Recommendation 4
We recommend that OPM test the security controls of [the major system] in accordance with the ISCMP testing schedule and ensure that the results are properly documented.

OPM Response: OPM concurs with the recommendation. After receipt of the draft report, OPM completed testing the security controls of the major system and documented the results according to OPM security procedures.

Recommendation 5
We recommend that OPM update the [the major system] contingency plan to include all required Information from OPM's template.

OPM Response: OPM concurs with the recommendation. OPM is in the process of updating the major system contingency plan.

Recommendation 6
We recommend that OPM update the [the major system] POA&M to include all identified weaknesses and required information per OPM policy.

OPM Response: OPM concurs with the recommendation. OPM is in transition from one POA&M tracking tool to another. After receipt of the draft report, OPM added the POA&Ms to the new tracking tool. The POA&Ms are now in the process of being updated with the required information.

Recommendation 7
We recommend that OPM develop a detailed action plan to remediate all overdue POA&M items. This action plan should include realistic estimated completion dates.

OPM Response: OPM concurs with the recommendation. OPM is in the process of updating the POA&M items with new estimated completion dates, taking into consideration any factors that have led to the previously missed dates.

Recommendation 8
We recommend that OPM document the approved security configuration settings for [the major system].

OPM Response: OPM concurs with the recommendation. OPM will assess the risk of this finding and create an action plan to apply security controls to mitigate the identified risk, where appropriate.

Recommendation 9
We recommend that OPM develop and implement a plan to replace [the application] with a fully supported financial system.

OPM Response: OPM concurs with the recommendation. OPM has embarked upon an initiative to modernize the application. As a part of this effort, OPM is in the acquisition planning stage of assessing commercially available alternatives for systems implementation services, application hosting services, operational support (post implementation including help desk services), and Commercial Off-The-Shelf (COTS) financial management software applications. The objectives of the application replacement / Trust Funds Modernization effort are to modernize/replace the current system to facilitate greater transparency, compliance, and overall stability and sustainability of the system

Again, thank you for the opportunity to provide comment to this draft report. Please contact us or [redacted] if you have questions or need additional information.

cc:
[redacted]
Chief Information Security Officer

Mark W. Lambert
Associate Director, Merit Systems Accountability and Compliance

Janet L. Barnes
Director, Internal Oversight and Compliance

Jason D. Simmons
Chief of Staff

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