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 ELECTRONIC OFFICIAL PERSONNEL FOLDER SYSTEM

Report Number 4A-CI-00-20-007
June 30, 2020

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Electronic Official Personnel Folder System

Report No. 4A-CI-00-20-007 **June XX, 2020**

Why Did We Conduct The Audit?

The Electronic Official Personnel Folder (eOPF) has been identified as one of the Office of Personnel Management's (OPM) major systems. The Federal Information Security Modernization Act requires Inspectors General to complete annual evaluations of their respective agency's security programs and practices including testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems. Our audit consisted of an evaluation of the eOPF information technology (IT) security environment.

What Did We Audit?

The Office of the Inspector General completed a performance audit of eOPF 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 (OCIO).

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our system audit of eOPF determined that:

- The eOPF Authorization to Operate (ATO) was granted in July 2019 for three years. Nothing came to our attention to indicate that eOPF's ATO was inadequate.
- The eOPF Privacy Threshold Analysis from March 2020 accurately identified that a Privacy Impact Assessment (PIA) should be completed.
- The eOPF PIA has not had a documented review since September 2017.
- The eOPF Federal Information Processing Standards 199 accurately categorized the system as a "high" impact system.
- The eOPF System Security Plan was last updated in November 2019, adequately reflects the system's current state, and follows the required OCIO template.
- The Security Assessment Plan, Security Assessment Report, and Risk Assessment Table all accurately follow the appropriate templates, and include all the required sections for the documents.
- Continuous monitoring appears to be conducted in accordance with applicable policies and procedures.
- In April 2019, OPM moved the eOPF backup site from Macon, Georgia to Boyers, Pennsylvania. However, the eOPF Contingency Plan has not been updated to reflect the move and a new Contingency Plan test has not been conducted.
- The eOPF Plan of Action and Milestones had 12 open weaknesses that were accurately identified and tracked.
- The eOPF security controls tested appear to be in compliance with NIST SP 800-53, Revision 4.

ABBREVIATIONS

ATO	**Authorization to Operate**
Authorization	**Security Assessment and Authorization**
CISO	**Chief Information Security Officer**
eOPF	**Electronic Official Personnel Folder**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
OCIO	**Office of the Chief Information Officer**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
PIA	**Privacy Impact Assessment**
POA&M	**Plan of Action and Milestones**
PTA	**Privacy Threshold Analysis**
RAT	**Risk Assessment Table**
SAP	**Security Assessment Plan**
SAR	**Security Assessment Report**
SP	**Special Publication**
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.

According to the Electronic Official Personnel Folder's (eOPF) System Security Plan (SSP), eOPF provides federal agencies a history of electronic personnel records regarding individuals working for the federal government. eOPF is one of the agency's major information technology (IT) systems, and as such, FISMA requires that the Office of the Inspector General (OIG) perform an audit of IT security controls of this system.

This was our second audit of eOPF. The previous audit is documented in Report 4A-HR-00-09-032, dated June 2, 2009. There were no recommendations from the previous audit.

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

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Our objective was to perform an audit of the security controls for eOPF 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 eOPF, 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 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 eOPF, including the evaluation of IT security controls in place as of March 2020.

We considered the eOPF 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 with security responsibilities for eOPF, 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 eOPF 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 eOPF internal controls taken as a whole. The criteria used in conducting this audit include:

- OPM Security Assessment and Authorization Guide;
- OPM Plan Of Action And Milestones Guide;
- OPM Contingency Planning 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 800-30, Revision 1, Guide for Conducting Risk Assessments;
- 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;

- NIST SP 800-37, Revision 2, Information Security Continuous Monitoring for Federal Information Systems and Organizations; 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 November 2019 through March 2020 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 eOPF 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

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, a current Authorization is required for every OPM system.

OPM management granted eOPF an authorization to operate (ATO) in July 2019. The ATO is valid for up to three years and includes provisions that the system owner monitor and remediate identified weaknesses on an ongoing basis.

eOPF was granted an ATO in July 2019.

Nothing came to our attention to indicate that the eOPF's ATO was inadequate.

B. FIPS 199 ANALYSIS

The E-Government Act of 2002 requires Federal agencies to categorize all Federal information and information systems. Federal Information Processing Standards (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, provides an overview of the security objectives and impact levels identified in FIPS 199.

The eOPF security categorization documentation analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. eOPF is categorized as a "high" impact level for each area – confidentiality, integrity, and availability – resulting in an overall categorization of "high."

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

Nothing came to our attention to indicate that the eOPF 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. A Privacy Threshold Analysis was performed on eOPF in March 2020, and it was determined that a Privacy Impact Assessment was required for this system. According to the Office of Privacy and Information Management, the current eOPF PTA expires in March 2021.

OMB Memorandum M-03-22 outlines the necessary components of a PIA. The purpose of the assessment is to evaluate and document any personally identifiable information maintained by an information system. The eOPF PIA was completed and was formally approved and signed by the Chief Privacy Officer in September 2017. However, OPM has not provided evidence of a subsequent review and approval.

OPM's Information Systems Privacy Policy states that the System Owner "shall review their PTA and PIA (if applicable) at least annually and document whether there are any changes to the system as required by Federal Information Security Management Act (FISMA) reporting."

Failure to routinely update the PIA can mislead the System Owner, Chief Information Security Officer (CISO), and Authorizing Official on the overall privacy impact of the system.

Recommendation 1

We recommend that OPM review the eOPF PIA in accordance with agency policy and document the conclusion of the review.

OPM Response:

"We do not concur. A Privacy Impact Assessment (PIA) for the eOPF system was completed and signed in September 2017 and, absent any significant changes, will be updated in September 2020, consistent with Office of Management and Budget (OMB) guidance and OPM policy and practice.

On page 6 of your draft report, it states that 'a Privacy Threshold Analysis (PTA) was performed on eOPF in March 2020, and it was determined that a PIA was required for this system.' A similar statement exists on the 'What did we find' page at the beginning of your draft report. While it is correct that an updated PTA was completed for the eOPF system in March 2020 and that the PTA notes that a PIA is required for the system, it does not require,

as the draft report implies, that a new PIA be completed. The PTA is simply stating that the system requires a PIA; the required PIA was completed in September 2017. The PTA is used to document annually, or at any point when a change is made to the system, whether any change impacts the privacy impact assessment documented in the PIA and requiring an update. The March 2020 PTA update documents the movement of the backup redundant system and notes that no PIA update is required at this time. The PTA explicitly states that there have been no significant changes to the system since the last PTA update and therefore the current PIA will remain in effect."

OIG Comment:

We acknowledge that there have been no significant privacy changes to the eOPF system since the previous PTA dated September 17, 2018, and that the March 2020 PTA specifically states the current PIA will remain in effect. However, as mentioned above, OPM's 2011 Information Security and Privacy Policy Handbook requires that the System Owner "shall review their PTA and PIA (if applicable) at least annually and document whether there are any changes to the system as required by Federal Information Security Management Act (FISMA) reporting." Based on the nature of OPM's response, we believe that there may be some confusion due to the wording of the recommendation. The intent of the recommendation is for the PIA to be reviewed annually, and for the conclusion of the review to be documented even if no changes were made. We will therefore modify the wording of the recommendation to add clarity since we have not received any evidence that the PIA has been reviewed since it was created in 2017.

We recommend that the OCIO review the PIA annually in accordance to OPM policy, and document the conclusion of the review.

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 an SSP for each system, and provides guidance for doing so.

The OCIO developed the eOPF SSP using the OCIO SSP template, which uses the 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;
- Minimum Security Controls;
- Security Control Selection;
- Completion and Approval Dates; and
- Laws, Regulations, and Policies Affecting the System.

We reviewed the current eOPF SSP, last updated in November 2019, and determined that it adequately reflects the system's current state, and follows the required SSP template.

Nothing came to our attention to indicate that the eOPF SSP has not been properly documented and approved.

E. SECURITY ASSESSMENT PLAN AND REPORT

A Security Assessment Plan (SAP) describes the scope, procedures, environment, team, roles, and responsibilities for an assessment to determine the effectiveness of a system's security controls. The Security Assessment Report (SAR) presents the results of the Security Assessment Plan and includes a review of management, operational and technical security controls. The Risk Assessment Table (RAT) maintains the list of individual security controls associated with the system, including the likelihood of harm and the potential threat impact to the agency. We reviewed these documents to verify that a risk assessment was conducted in accordance with NIST SP 800-30, Revision 1. We also verified that appropriate management, operational, and technical controls were tested for a system with a "high" security categorization.

OCIO completed the eOPF SAP in February 2019, the eOPF SAR in April 2019, and the eOPF RAT in November 2019. The SAP, SAR, and RAT all accurately follow the appropriate templates, and include all the required sections for the documents.

Nothing came to our attention to indicate that the eOPF SAP, SAR, and RAT 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 received the FY 2019 quarterly continuous monitoring submissions for eOPF. Our review of the submissions revealed that there are 386 total controls. Of those 386 controls, 181 are listed as fully satisfied, 19 are not satisfied, 20 are partially satisfied, and 166 were listed as not applicable for various reasons (e.g., controls inherited from another system).

Nothing came to our attention to indicate that the eOPF 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 OPM CISO directed the eOPF production systems to be placed in OPM's Macon, Georgia data center and the backup systems to be placed at an Iron Mountain facility in Boyers, Pennsylvania when the system migrated from the U.S. Department of Interior to OPM in 2017. However, due to a lack of space at the Iron Mountain facility, OPM placed both the production and backup systems in the Macon data center from July 2017 to April 2019, even though NIST SP 800-34, Revision 1, advises against having the production and backup systems in the same location. The eOPF Contingency Plan was developed in July 2018.

In April 2019, OPM was able to move the eOPF backup systems to Boyers, Pennsylvania as originally planned. However, the eOPF Contingency Plan has not been updated to reflect the change in backup location.

The eOPF Contingency Plan does not reflect an accurate location of the backup site.

According to OPM's Contingency Planning Policy, the System Owner should "Update the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing."

Failure to update a system contingency plan can cause confusion and exacerbate outages during an incident.

Recommendation 2

We recommend that OPM update the eOPF Contingency Plan in accordance with OPM policies.

OPM Response:

"***We concur. We will update the contingency plan to reflect the current location of the backup site."***

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. This statement also applies to all subsequent recommendations in this audit report that the OCIO agrees to implement.

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, also provides guidance for testing contingency plans and documenting the results.

The eOPF Contingency Plan was last tested in November 2018. The test showed satisfactory results for all OPM Macon data center eOPF applications. However, no contingency plan

test was conducted in FY 2019. The potential consequences of not performing the contingency plan test in FY 2019 are compounded by the fact that the backup systems were recently moved and no testing has been performed to ensure that eOPF can be restored at the new location.

According to OPM's Contingency Planning Policy, the contingency plan test should be conducted annually.

Failure to conduct an annual contingency plan test can lead to ineffective response time during a disaster, and potentially exacerbate system outages.

Recommendation 3

We recommend that OPM conduct a test of the updated eOPF Contingency Plan in accordance with OPM policies. Note: This recommendation cannot be implemented until the Contingency Plan is updated as a part of the corrective action for Recommendation 2.

OPM Response:

"We concur. We will conduct a contingency plan test of the updated eOPF Contingency Plan in accordance with OPM policies."

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.

During the audit, we found that eOPF had 12 open weaknesses that were accurately identified and tracked in accordance with the OPM Plan of Actions and Milestone Guide. The eOPF POA&M is also properly formatted according to OPM policy.

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

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 OPM has implemented a subset of these controls for eOPF. We tested approximately 26 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;
- Physical and Environmental Protection;
- Risk Assessment;
- Security Planning;
- Security Assessment and Authorization;
- System and Communications Protection;
- System Maintenance; and
- System and Information Integrity.

The control selection process began by eliminating controls that were reflected on the eOPF POA&M. We also removed controls that were considered agency common controls and controls inherited from other systems from consideration. From the remaining controls, we made a risk-based decision and selected our sample.

These specific controls were evaluated by interviewing individuals with system security responsibilities, reviewing documentation and system screenshots, and viewing demonstrations of system capabilities.

We determined that the security controls and/or control enhancements tested appear to be in compliance with NIST SP 800-53, Revision 4.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Chief Information
Officer

May 1, 2020

MEMORANDUM FOR: [redacted]
Chief, Information Systems Audits Group

FROM: Clare A. Martorana
Chief Information Officer

Cord E. Chase
Chief Information Security Officer

SUBJECT: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Electronic Official Personnel Folder (Report No. 4A-CI-00-20-007)

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 the U.S. Office of Personnel Management's Electronic Official Personnel Folder (eOPF), Report No. 4A-CI-00-20-007.

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

Recommendation #1: We recommend that OPM update the eOPF PIA document accordance with agency policy.

Management Response: We do not concur. A Privacy Impact Assessment (PIA) for the eOPF system was completed and signed in September 2017 and, absent any significant changes, will be updated in September 2020, consistent with Office of Management and Budget (OMB) guidance and OPM policy and practice.

On page 6 of your draft report, it states that "a Privacy Threshold Analysis (PTA) was performed on eOPF in March 2020, and it was determined that a PIA was required for this system." A similar statement exists on the "What did we find" page at the beginning of your draft report. While it is correct that an updated PTA was completed for the eOPF system in March 2020 and that the PTA notes that a PIA is required for the system, it does not require, as the draft report implies, that a new PIA be completed. The PTA is simply stating that the system requires a PIA; the required PIA was completed in

September 2017. The PTA is used to document annually, or at any point when a change is made to the system, whether any change impacts the privacy impact assessment documented in the PIA and requiring an update. The March 2020 PTA update documents the movement of the backup redundant system and notes that no PIA update is required at this time. The PTA explicitly states that there have been no significant changes to the system since the last PTA update and therefore the current PIA will remain in effect.

Recommendation #2: We recommend that OPM update the eOPF Contingency Plan in accordance with OPM policies.

Management Response: We concur. We will update the contingency plan to reflect the current location of the backup site.

Recommendation #3: We recommend that OPM conduct a test of the updated eOPF Contingency Plan in accordance with OPM policies. Note: This recommendation cannot be implemented until the Contingency Plan is updated as a part of the corrective action for Recommendation 2.

Management Response: We concur. We will conduct a contingency plan test of the updated eOPF Contingency Plan in accordance with OPM policies.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact [redacted], [redacted], or [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