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 WHITE HOUSE FELLOWS SYSTEM

Report Number 2024-ISAG-009
August 8, 2024

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's White House Fellows System

Report No. 2024-ISAG-009 **August 8, 2024**

Why Did We Conduct the Audit?

The Federal Information Security Modernization Act (FISMA) requires Inspectors General to complete annual evaluations of their respective agency's security programs and practices, which includes testing the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems. The White House Fellows (WHF) system was selected to include in this year's representative subset of systems because it is one of the U.S. Office of Personnel Management's (OPM) moderate risk, major systems, and an audit of its information technology (IT) security controls has not been performed within the past 10 years.

What Did We Audit?

The OPM Office of the Inspector General completed a performance audit of the WHF system's IT security controls to ensure that they have been implemented in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), and the OPM Office of the Chief Information Officer (OCIO).

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the WHF system's IT security controls concluded that:

- The WHF system's security categorization is compliant with NIST Special Publication (SP) 800-53, Revision 5, control RA-2 Security Categorization.
- We agree with the WHF's privacy threshold analysis conclusion that the system does require a privacy impact assessment.
- The WHF system's Security Plan is complete and follows the OCIO's template.
- The WHF's security and risk assessments are compliant with NIST SP 800-53, Revision 5, controls RA-3 Risk Assessment and CA-2 Control Assessments.
- Continuous Monitoring for the WHF system was conducted in accordance with OPM's quarterly schedule for fiscal year 2024.
- The WHF system's contingency plan was completed in accordance with NIST SP 800-34, Revision 1, and OCIO guidance.
- The WHF system's Plan of Action and Milestones documentation is up to date and contains all identified weaknesses.
- The WHF system received an ongoing Authorization to Operate in December 2022.
- We evaluated a subset of the system controls outlined in NIST SP 800-53, Revision 5. We determined 39 out of the 40 controls of the WHF system are in compliance.

ABBREVIATIONS

ATO	**Authorization to Operate**
BIA	**Business Impact Analysis**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
HVA	**High Value Asset**
ISCM	**Information Security Continuous Monitoring**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
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 Assessment**
P.L.	**Public Law**
POA&M	**Plan of Action and Milestones**
PTA	**Privacy Threshold Analysis**
SORN	**System of Records Notice**
SP	**Special Publication**
SSP	**System Security Plan**
WHF SYSTEM	**White House Fellows System**

TABLE OF CONTENTS

I. BACKGROUND

On December 17, 2002, President George W. Bush signed Public Law (P.L.) 107-347, the E-Government Act, into law, which included Title III, the Federal Information Security Management Act (FISMA). FISMA requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting of the results of IG evaluations for unclassified systems to the U.S. Office of Management and Budget (OMB), and (4) an annual OMB report to Congress summarizing the material received from agencies.

In 2014, P.L. 113-283, the Federal Information Security Modernization Act, was established and reaffirmed the objectives of the Federal Information Security Management Act. FISMA states that each year, each agency shall have an independent evaluation of its information security program and practices to determine their effectiveness. Evaluations shall include testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems. Agencies with an IG appointed under the Inspector General Act of 1978, as amended (5 U.S.C. §§ 401-424), shall have the evaluation performed by the IG of the agency or by an independent external auditor, as determined by the IG of the agency.

According to the White House Fellows (WHF) system's security plan (SSP), the system is owned by the Executive Office of the President's Commission on White House Fellowships and is managed by the U.S. Office of Personnel Management's (OPM) Human Resources Solutions Information Technology Program Management Office. The web site allows for applicants to complete an application online and provide the Executive Office of the President's Commission with the application package to use for selecting candidates for a yearlong government fellowship position.

The WHF system has been included in this year's representative subset of systems to be evaluated because it is one of OPM's moderate risk, major systems, and an audit of its information technology (IT) security controls has not been performed within the past 10 years.

II. OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The objective of this audit was to determine if the OPM Office of the Chief Information Officer (OCIO) has implemented IT security controls for the WHF system in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), and the OPM OCIO.

SCOPE AND METHODOLOGY

The scope of this audit included IT security controls defined by FISMA, NIST, and OPM OCIO policies, which impact the IT security posture of the WHF system as of May 2024.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, issued by the U.S. Comptroller General. Generally Accepted Government Auditing Standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Accordingly, the audit included an evaluation of related policies and procedures, control tests, and other auditing procedures we considered necessary to achieve our objective.

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

- Security Categorization;
- Privacy Impact Assessment (PIA);
- System Security Plan;
- Security and Risk Assessments;
- Continuous Monitoring;
- Plan of Action and Milestones (POA&M);
- Authorization Memo;
- Contingency Planning; and
- NIST Special Publication (SP) 800-53, Revision 5, Security Controls.

Control tests were performed to determine the extent to which established controls and procedures are functioning as intended. NIST SP 800-53A, Revision 5, Assessing Security and Privacy Controls in Information Systems and Organizations, includes a comprehensive set of procedures for assessing the effectiveness of security and privacy controls defined in NIST SP 800-53, Revision 5. We used these potential assessment methods and artifacts, where appropriate, to evaluate the WHF system's controls. This included interviews, observations, tests, and examination of computer-generated data and various documents including IT and other related organizational policies and procedures. Where appropriate, control tests utilized

judgmental sampling methods. Results of judgmentally selected samples cannot be projected to the entire population since it is unlikely that the results are representative of the population as a whole.

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 during this audit caused us to doubt the reliability of the computer-generated data used. We believe that the data was sufficient to achieve the audit objectives.

We considered the WHF system's 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. Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the WHF system's internal controls taken as a whole.

The OPM Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended (5 U.S.C. §§ 401-424), performed the audit. The OPM OIG conducted the audit remotely from OPM's Jacksonville, Florida and Washington, D.C. offices between December 2023 and May 2024.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting this audit, various laws, regulations, and industry standards were used as criteria to evaluate the WHF system's control structure. These criteria included, but were not limited to, the following publications:

- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- Federal Information Security Modernization Act of 2014 (P.L. 113-283);
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60, Revision 2, Guide for Mapping Types of Information and Systems to Security Categories;
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems;

- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems;
- OMB Circular A-130, Managing Information as a Strategic Resource;
- OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act; and
- OPM OCIO's IT security policies and procedures.

While generally compliant with respect to the items tested, OPM was not in compliance with all standards, as described in section III of this report, "Audit Findings and Recommendation."

III. AUDIT FINDINGS AND RECOMMENDATION

A. SECURITY CATEGORIZATION

The WHF System's security categorization is moderate.

OMB Circular A-130, Managing Information as a Strategic Resource, requires federal agencies to assign a security categorization to all federal information and information systems. To adhere to OMB Circular A-130 requirements for security categorizations of information systems, OPM follows the standards and guidelines defined in the FIPS Publication 199 and NIST SP 800-60. The FIPS Publication 199 defines standards to be used by federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to risk. NIST SP 800-60 has been developed to provide guidelines to federal agencies to categorize information and information types. In addition to the security categorization process, OMB M-19-03 establishes how agencies determine if a system is a High Value Asset (HVA). To ensure that OPM systems are satisfying security categorization requirements outlined by FIPS, NIST, and OMB, OPM has developed templates for FIPS 199 Security Categorization and HVA evaluations.

The WHF system's security categorization document includes an analysis of the impact that will result from a loss of system and information confidentiality, availability, and integrity. OPM categorized the WHF system as a "moderate" impact level for confidentiality, integrity, and availability. In accordance with FIPS Publication 199, OPM used the maximum potential impact value to assign the WHF system's overall security categorization as "moderate." OPM's security categorization is consistent with FIPS Publication 199 requirements.

OPM's HVA evaluation of the WHF system was conducted using OPM's HVA Worksheet, which is based on OMB guidelines and provides instructions for conducting the evaluation. OPM's HVA evaluation determined that the WHF system is a mission essential system which contains sensitive information but is not an HVA system. Our review of the WHF system's HVA Worksheet concluded that OPM followed the required guidance documented in the HVA Template and correctly classified the WHF system.

No opportunities for improvement related to the WHF system's security categorization were identified.

B. PRIVACY IMPACT ASSESSMENT

The WHF system is designated as a privacy sensitive system and does require a PIA.

The E-Government Act of 2002 requires federal agencies to perform a PIA for systems that collect, maintain, or disseminate information that is in an identifiable form. The PIA should address privacy-related concerns including, but not limited to, what information is to be collected; why the information is being collected; with whom the information will be shared; and how the information will be secured. A privacy

threshold analysis (PTA) documents the continuous monitoring of privacy risk and mitigation for the system and is used to determine whether a system requires a PIA.

The WHF system's PTA was last updated June 27, 2022, and concluded that the WHF system does require a PIA because it is designated as a privacy sensitive system. In accordance with OPM procedure, the PTA's designation was reviewed and reapproved by a designee of OPM's Chief Privacy Officer before the PTA's expiration date. Our review of the WHF system's PIA, which was last updated on May 10, 2024, concluded that the requirements of NIST SP 800-53, Revision 5, control RA-8 have been adequately implemented.

No opportunities for improvement related to the WHF system's privacy impact assessment were identified.

C. SYSTEM SECURITY PLAN

OMB Circular A-130 requires federal agencies to implement, for each information system, the security controls outlined in NIST SP 800-53, Revision 5, 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, provides guidance for developing and documenting security controls in the SSP.

The OCIO developed the WHF system's 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 WHF system's SSP, last updated in December 2023, and determined that it adequately reflects the system's current state. No opportunities for improvement related to the WHF system's SSP were identified.

D. SECURITY AND RISK ASSESSMENTS

OMB Circular A-130 requires that federal agencies "Conduct and document assessments of all selected and implemented security and privacy controls to determine whether security and privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable requirements and to manage security and privacy risks … ." For the Authorizing Official to grant a system an Authorization to Operate (ATO), the Authorizing Official must receive essential information about the security posture of the system, which includes security control assessment results.

According to the OPM Security Authorization Guide, the security assessment plan describes a security assessment's scope and procedures. Using the security assessment plan, an assessment of the system's implemented security controls will be performed. The results of the assessment will be included in the assessment results table. Using the assessment results table, the Information System Security Officer documents a risk assessment for all identified weaknesses in a risk assessment table. All the residual risks remaining in the system are summarized in a risk assessment report which is presented to the Authorizing Official to review before making an authorization decision.

OPM tests all of a system's applicable controls over a three-year period. A subset of controls are tested at least triennially during an independent security controls assessment. The remaining controls are tested as part of the system's continuous monitoring activities.

The WHF system's most recent security assessment plan was for an independent security controls assessment conducted in June 2022. The test results were documented in an assessment results table, and a risk assessment of identified weaknesses was documented in a risk assessment table. The residual risks remaining in the system were captured within the WHF system's risk assessment report document and included corrective actions that were recorded in the WHF system's POA&Ms.

All requirements of NIST SP 800-53, Revision 5, controls CA-2 and RA-2 have been adequately implemented by the WHF system's security and risk assessments.

No opportunities for improvement related to the WHF system's security and risk assessments were identified.

E. CONTINUOUS MONITORING

OMB Circular A-130 requires federal agencies to develop and implement an information security continuous monitoring (ISCM) strategy. ISCM is the maintenance of ongoing awareness of information security, vulnerabilities, and threats to support an agency's ability to manage risk. The ISCM strategy must define the degree of rigor and the frequency at which all controls selected to implement for the system are evaluated.

OPM's Continuous Monitoring Policy requires the Chief Information Security Officer to develop a continuous monitoring strategy and implement a continuous monitoring program to be conducted at least quarterly. Evidence was provided by OPM that demonstrated continuous monitoring for fiscal year 2024.

Our review of the WHF system's authorization memorandum demonstrated that OPM is adhering to the following requirements of NIST SP 800-53, Revision 5, control CA-7:

- Established system-level metrics to be monitored;
- Established organization-defined frequencies for monitoring and for assessment of control effectiveness;
- Correlated and analyzed information generated by control assessments and monitoring; and
- Addressed the results of the control assessments analysis with response actions.

No opportunities for improvement related to the WHF system's continuous monitoring were identified.

F. CONTINGENCY PLANNING

OPM adheres to NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems and OMB A-130, Managing Information as a Strategic Resource. NIST defines contingency planning as plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption.

As a part of the seven-step process to develop and maintain an effective information system contingency plan, NIST requires a business impact analysis (BIA) to be conducted. The purpose of the BIA is to correlate the system with the critical mission/business processes and services provided, and based on that information, characterize the consequences of a disruption. OPM has developed templates for both the BIA and Contingency Plan to ensure the organization is adhering to NIST requirements.

Additionally, OPM follows policies, which require the agency to conduct a review/test of contingency plans for information systems at least annually. Testing of contingency plans shall include a review of test results and the initiation of corrective actions if needed.

The WHF system's contingency plan satisfies requirements of NIST SP 800-53, Revision 5, controls CP-2 and CP-4 which include:

- Identifying essential mission and business functions;
- Providing recovery objectives, restoration priorities, and metrics; and
- Incorporating lessons learned from contingency plan testing.

No opportunities for improvement related to the WHF system's contingency planning were identified.

G. 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 WHF system has three open POA&Ms with weaknesses identified that need to be remediated. The risk level for the POA&Ms is low and medium, and all weaknesses are properly documented and include attainable closure dates. The WHF system 's POA&Ms are properly formatted and adhere to OPM's policies and procedures.

No opportunities for improvement related to the WHF system's POA&Ms were identified.

H. AUTHORIZATION MEMORANDUM

OMB Circular A-130 requires all federal information systems to have a valid ATO. An authorization memo is an official management decision to authorize a system to operate and accept its known risks.

The WHF system received an ongoing ATO in December 2022. The decision does not include an authorization termination/expiration date. During ongoing authorization, risks are monitored against OPM's risk tolerance on an ongoing basis. The authorization is contingent upon continuing to manage risk in accordance with the Cybersecurity Risk Management Strategy and fulfilling responsibilities specified in the authorization memo.

These responsibilities include:

- Continued mitigation and/or remediation of any open Plan of Action and Milestones with reasonable completion dates and milestones; and

- Documentation and submission of required continuous monitoring artifacts as outlined in OPM's Information Security Continuous Monitoring Plan.

Our review of the WHF system's authorization memorandum also demonstrated that OPM is adhering to the following requirements of NIST SP 800-53, Revision 5, control CA-6:

- A senior official has been assigned as the Authorizing Official for the WHF system;

- The ATO for the WHF system has been updated within OPM's defined frequency; and

- The Authorizing Official for common controls authorized the use of those controls for inheritance by organizational systems.

No opportunities for improvement related to the WHF system's ATO were identified.

I. NIST SP 800-53 CONTROLS TESTING

NIST SP 800-53, Revision 5, 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.

The WHF system adequately implemented 39 of the 40 controls tested.

Out of a total of 286 NIST SP 800-53, Revision 5, controls that are applicable to the WHF system, we judgmentally selected a sample of 40 to test of which 39 were adequately implemented. Our judgmental sample was selected from high-risk areas identified during the planning phase of this audit and includes controls related to system authorization documentation; vulnerability and configuration management; and all controls that are fully implemented by the system (i.e., system-specific controls). One or more controls from each of the following control families were tested:

- Access Control;
- Configuration Management;
- Maintenance;
- System and Communications Protection;
- System and Services Acquisition
- Audit and Accountability;
- Contingency Planning;
- Planning;
- System and Information Integrity; and

These controls were evaluated by reviewing documentation and system screenshots and viewing demonstrations of system capabilities.

However, we identified the following opportunities for improvement related to the WHF system's controls testing.

1. Controls Testing – SI-12

We performed controls testing on 40 of the WHF system-specific controls. As a result of our controls testing, we determined that OPM had a deficiency in one of the controls.

For control SI-12, within Archer and the WHF system's Privacy Threshold Analysis, OPM stated that the WHF system's System of Records Notice (SORN) is under development.

NIST SP 800-53, Revision 5, control SI-12 states that the agency "Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements."

NIST SP 800-53, Revision 5, control PT-6 states that the agency "Publish system of records notices in the Federal Register; and Keep system of records notices accurate, up-to-date, and scoped in accordance with policy."

Office of Management and Budget, Circular No. A-108, Publishing System of Records Notices, states that "The Privacy Act requires agencies to publish a SORN in the Federal Register describing the existence and character of a new or modified system of records. A SORN is comprised of the Federal Register notice(s) that identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system."

Failure to publish a SORN with the most recent information about the system's records increases the risk that privacy violations could occur.

Recommendation 1

We recommend that OPM develop a SORN for the WHF system and publish the SORN in the Federal Register.

OPM's Response:

"We Concur. Our Office of the Executive Secretariat, Privacy, and Information Management agrees with the recommendation and will work with the White House

Fellows program and the Chief Information Office to further develop, finalize, and publish the System of Records Notice in the Federal Register."

OPM OIG Comment:

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

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

June 28, 2024

MEMORANDUM FOR: ERIC W. KEEHAN
Office of the Inspector General (OIG)
Chief, Information Systems Audits Group

FROM: KIRSTEN J. MONCADA
Executive Director, Office of the Executive Secretariat, Privacy, and Information Management

KIRSTEN MONCADA Digitally signed by KIRSTEN MONCADA Date: 2024.06.28 13:51:47 -04'00'

SUBJECT: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's White House Fellows System – FY 2024 (Report No. 2024-ISAG-009)

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 White House Fellows System – FY 2024 (Report No. 2024-ISAG-009)

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

Recommendation 1

We recommend that OPM develop a SORN for WHF and publish the SORN in the Federal Register

Management Response: Recommendation 1

We Concur. Our Office of the Executive Secretariat, Privacy, and Information Management agrees with the recommendation and will work with the White House Fellows program and the Chief Information Office to further develop, finalize, and publish the System of Records Notice in the Federal Register.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Marc Flaster, Deputy Executive Director, OESPIM, [redacted],[redacted]

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: https://oig.opm.gov/contact/hotline

By Phone: Toll Free Number: (877) 499-7295

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