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 ENTERPRISE MAINFRAME SYSTEM

Report Number 2023-ISAG-016
February 26, 2024

EXECUTIVE SUMMARY

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

Report No. 2023-ISAG-016 **February 26 , 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 Enterprise Mainframe (EM) 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 EM'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 EM's IT security controls did not result in any findings requiring recommendations. Our audit concluded that:

- EM's security categorization is compliant with NIST Special Publication) 800-53, Revision 5, control RA-2 Security Categorization.
- We agree with EM's privacy threshold analysis conclusion that EM does not require a privacy impact assessment.
- The EM System Security Plan was complete and follows the OCIO's template.
- EM's security and risk assessments are compliant with NIST Special Publication 800-53, Revision 5, control RA-3 Risk Assessment and CA-2 Control Assessments.
- Continuous Monitoring for EM was conducted in accordance with OPM's quarterly schedule for fiscal year 2023.
- The EM contingency plan was completed in accordance with NIST Special Publication 800-34, Revision 1, and OCIO guidance.
- EM's contingency plan test was last conducted in July 2023, and adheres to OPM's annual testing requirement.
- The EM Plan of Action and Milestones documentation is up to date and contains all identified weaknesses.
- A Security Assessment and Authorization was completed in October 2023, and is valid until February 2024. The Authorization is contingent upon fulfilling the responsibilities specified in the authorization memorandum.
- We evaluated a subset of the system controls outlined in NIST Special Publication 800-53, Revision 5. We determined that the security controls tested appear to be in compliance.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
EM	**Enterprise Mainframe System**
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**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
P.L.	**Public Law**

TABLE OF CONTENTS

I. BACKGROUND

On December 17, 2002, the President of the United States (U.S.) signed Public Law (P.L.) 107-347, the E-Government Act, into law, which included Title III, the Federal Information Security Management Act. It 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 (FISMA), 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 Enterprise Mainframe (EM) system security plan, EM assists the U.S. Office of Personnel Management (OPM) in meeting its goals by supporting information systems that serve OPM's principal Program Offices - Retirement Services, Healthcare and Insurance, the Office of the Chief Financial Officer, and administrative support systems. The EM Data Center's mainframe servers form a hybrid infrastructure supporting legacy information systems and new web-based systems on a single highly virtualized architecture.

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

We discussed the results of our audit with OPM representatives and provided a draft report to elicit their comments. As the draft report did not contain any formal recommendations, we did not receive any comments in response to the draft report.

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 EM 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 EM as of December 2023.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, issued by the U.S. Comptroller General. The 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 EM, including:

- Security Categorization;
- Privacy Impact Assessment;
- System Security Plan;
- Security and Risk Assessments;
- Continuous Monitoring;
- Plan of Action and Milestones;
- Authorization Memorandum;
- Contingency Planning; and
- NIST Special Publication 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 Special Publication 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 Special Publication 800-53, Revision 5. We used these potential assessment methods and artifacts, where appropriate, to evaluate EM'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 EM'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 EM'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 February 2023 and December 2023.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting this audit, various laws, regulations, and industry standards were used as criteria to evaluate EM'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 Special Publication 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST Special Publication 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations;
- NIST Special Publication 800-39, Managing Information Security Risk;
- NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations;

- 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 Memorandum 04-04, E-Authentication Guidance for Federal Agencies; and
- OPM OCIO's IT security policies and procedures.

In conducting the audit, we performed tests to determine whether OPM's management of EM is consistent with applicable standards. We determined that OPM was mostly in compliance with all standards as described in Section III of this report, and any items that were not in compliance were previously identified in EM's Plan of Action and Milestones' documentation.

III. AUDIT FINDINGS

A. SECURITY CATEGORIZATION

EM's security categorization is high.

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. FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, defines standards to be used by Federal agencies to make security categorization decisions with the objective of providing sufficient information security controls according to risk. A system's minimum information security requirements are defined in FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, and are determined based on the security categorization it's assigned using FIPS Publication 199 guidance.

EM'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 EM as a "high" impact level for confidentiality and integrity, and a "moderate" impact level for availability. In accordance with FIPS Publication 199, OPM used the maximum potential impact value to assign EM's overall security categorization as "high."

EM's security categorization is consistent with FIPS Publication 199 requirements. OPM has adequately implemented the requirements of NIST Special Publication 800-53, Revision 5, control RA-2 Security Categorization.

No opportunities for improvement related to EM's security categorization were identified.

B. PRIVACY IMPACT ASSESSMENT

EM does not require a privacy impact assessment.

The E-Government Act of 2002 requires Federal agencies to perform a Privacy Impact Assessment for systems that collect, maintain, or disseminate information that is in an identifiable form. The Privacy Impact Assessment 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 documents the continuous monitoring of privacy risk and mitigation for the system and is used to determine whether a system requires a Privacy Impact Assessment. EM's privacy threshold analysis was last updated in April 2023 and concluded that EM does not require a Privacy Impact Assessment because it is not designated as a privacy sensitive system. In accordance with OPM procedure, the privacy threshold analysis' designation was reviewed and reapproved by a designee of OPM's Chief Privacy Officer before the privacy threshold analysis' expiration date. Since EM is not a privacy sensitive system, the requirements of NIST SP 800-53, Revision 5, control RA-8 Privacy Impact Assessments, have been adequately implemented.

No opportunities for improvement related to EM's Privacy Impact Assessment were identified.

C. SYSTEM SECURITY PLAN

Federal agencies must implement, for each information system, the security controls outlined in NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in a system security plan for each system, and provides guidance for doing so.

The OCIO developed the EM system security plan using the OCIO's system security plan template, which uses NIST Special Publication 800-18, Revision 1, as guidance. The template requires the system security plan 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 EM system security plan, last updated in May 2023, and determined that it adequately reflects the system's current state. Nothing came to our attention to indicate that the EM system security plan has not been properly documented and approved.

D. SECURITY AND RISK ASSESSEMENTS

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, 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 is tested triennially during an independent security controls assessment. The remaining controls are tested as part of the system's continuous monitoring activities.

EM's most recent security assessment plan was part of an independent security controls assessment that was conducted in August 2023. The 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 in a risk assessment report and shared with EM's Authorizing Official. We also reviewed continuous monitoring activities completed within the triennial period and verified that an acceptable portion of the system's applicable controls were tested.

All requirements of NIST Special Publication 800-53, Revision 5, control CA-2 Control Assessments and RA-2 Risk Assessment have been adequately implemented by EM's security and risk assessments.

No opportunities for improvement related to EM'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 strategy. Information security continuous monitoring is the maintenance of ongoing awareness of information security, vulnerabilities, and threats to support an agency's ability to manage risk. The information security continuous monitoring 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 completed at least quarterly. Evidence was provided by OPM that demonstrated continuous monitoring for fiscal year 2023.

Our review of EM's authorization memo demonstrated that OPM is adhering to the following requirements of NIST Special Publication 800-53, Revision 5, control CA-7 Continuous Monitoring:

- Correlation and analysis of information generated by control assessments and monitoring;
- Response actions to address results of the analysis of control assessments;
- Established system level metrics to be monitored; and
- Establishing organization defined frequencies for monitoring and assessment of control effectiveness.

No opportunities for improvement related to EM's continuous monitoring were identified.

F. CONTINGENCY PLANNING

NIST Special Publication 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 Review

The EM contingency plan, last updated in October 2023, documents the functions, operations, and resources necessary to restore and resume the system when unexpected events or disasters occur. The contingency plan also ensures coordination with external points of contact and vendors associated with EM. The contingency plan follows the format suggested by NIST Special Publication 800-34, Revision 1, and OPM's template for contingency plans.

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

2) Business Impact Analysis

OMB Circular A-130 requires that contingency plans for Federal information systems identify essential missions and business functions and associated contingency requirements. This is accomplished by performing a business impact analysis, which is a key component of the contingency planning process. The purpose of the business impact analysis is to correlate the system with the mission and business processes that it supports and use that information to describe the consequences of a service-impacting incident affecting the system.

The EM business impact analysis identified EM's functionality as providing a secure platform for the development, testing, and hosting of OPM's offices of Retirement Services, as well as the Healthcare and Insurance, Office of the Chief Financial Officer, and administrative support systems. The most recent EM business impact analysis was completed February 2023, and is within the required three-year cycle.

During our review of EM's business impact analysis, we did not identify any opportunities for improvement.

3) 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 Special Publication 800-34, Revision 1, provides guidance for testing contingency plans and documenting the results.

The contingency plan and test were completed in accordance with NIST guidance.

The EM contingency plan test was conducted in July 2023. The tabletop test consisted of a malicious actor compromising the EM Resource Access Control Facility credentials of a nonprivileged user. The test was considered successful, although there were lessons learned with booting and revoking access when the system detects malicious actors. There will not be a contingency plan test finding or recommendation in this report based on the lessons learned.

Nothing else came to our attention to indicate that the EM contingency plan testing process was inadequate.

G. PLAN OF ACTION AND MILESTONES PROCESS

A Plan of Action and Milestones 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 Plan of Action and Milestones process to help track known IT security weaknesses associated with the Agency's information systems.

There are two open Plan of Action and Milestones for EM with issues identified that need to be remediated. The risk level for the Plan of Action and Milestones is low and high, and all weaknesses are properly documented to include attainable closure dates. The EM Plan of Action and Milestones is properly formatted according to OPM policy.

We did not detect any issues with the EM Plan of Action and Milestones.

H. AUTHORIZATION MEMORANDUM

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

EM received an Authorization to Operate in October 2023. The authorization is valid until February 2024, and is contingent upon continuing to manage risk with the Cybersecurity Risk Management Strategy and fulfilling the 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;
- Documentation and submission of required continuous monitoring artifacts as outlined in OPM's Information Security Continuous Monitoring Plan; and
- Implementation of phishing resistant multifactor authentication by December 31, 2023, for EM components.

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

- A senior official has been assigned as the Authorizing Official for EM;
- The Authorization to Operate for EM has been updated within OPM's defined frequency; and
- The Authorizing Official has authorized the system to operate.

No opportunities for improvement were identified related to EM's Authorization Letter/Memorandum.

I. NIST SP 800-53 CONTROLS TESTING

NIST Special Publication 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.

EM adequately implemented all 34 of the controls we tested.

Out of a total of 325 NIST Special Publication 800-53, Revision 5, controls that are applicable to EM, we judgmentally selected a sample of 34 to test. 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;

Audit and Accountability;

Configuration Management;

Contingency Planning;

Maintenance;

Planning;

System and Communications Protection;

System and Information Integrity; and

System and Services Acquisition.

These controls were evaluated by interviewing individuals with system security responsibilities, reviewing documentation and system screenshots, and viewing demonstrations of system capabilities. Our tests concluded that all of the 34 controls assessed during this audit have been adequately implemented and appear to be in compliance with NIST Special Publication 800-53, Revision 5, requirements.

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