U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS AND EVALUATIONS

Final Audit Report

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Freedom of Information Act Xpress System

Report Number 2025-ISAG-024
June 8, 2026

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Freedom of Information Act Xpress System

Report No. 2025-ISAG-024 **June 8, 2026**

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. These evaluations include testing the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems. The Freedom of Information Act Xpress (FOIAXpress) system was selected to be included in this year's representative subset of systems because it is one of the U.S. Office of Personnel Management's (OPM's) moderate risk, major systems, and an audit of its information technology (IT) security controls has not previously been performed.

What Did We Audit?

The OPM Office of the Inspector General completed a performance audit of FOIAXpress' 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.

Matthew R. Knupp

Matthew R. Knupp
Acting Deputy Assistant Inspector General for Audits

What Did We Find?

Our audit of FOIAXpress' IT security controls concluded that:

- The FOIAXpress security categorization is compliant with NIST Special Publication (SP) 800-53, Revision 5, control RA-2 Security Categorization.
- The FOIAXpress privacy threshold analysis accurately concluded that a privacy impact assessment was required. No opportunities for improvement related to the privacy impact assessment were identified.
- The FOIAXpress System Security and Privacy Plan is complete and follows the Office of the Chief Information Officer's (OCIO) template.
- The FOIAXpress 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 FOIAXpress was adequately conducted.
- The FOIAXpress Plan of Action and Milestones documentation is up-to-date and contains all identified weaknesses.
- The FOIAXpress authorization to operate memorandum was not completed by the current authorizing official.
- The FOIAXpress contingency plan was completed in accordance with NIST SP 800-34, Revision 1, and OCIO guidance.
- We evaluated a subset of NIST SP 800-53, Revision 5, system controls and determined that all the controls we tested are adequately implemented.

ABBREVIATIONS

AO	**Authorizing Official**
ATO	**Authorization to Operate**
BIA	**Business Impact Analysis**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
FOIA	**Freedom of Information Act**
FOIAXpress	**Freedom of Information Act Xpress**
GAGAS	**Generally Accepted Government Auditing Standards**
GRC	**Governance, Risk, and Compliance**
IG	**Inspector General**
IG Act	**Inspector General Act of 1978, as amended, 5 U.S.C. §§ 401-424**
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**
SAP	**Security Assessment Plan**
SP	**Special Publication**
SPP	**System Security and Privacy Plan**
U.S.	**United States**

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 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 (IG Act), 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 Freedom of Information Act Xpress (FOIAXpress) System Security and Privacy Plan (SPP), FOIAXpress is a cloud-based software as a service application that provides tracking, management, and reporting of the entire lifecycle of the Freedom of Information Act (FOIA) and Privacy Act requests and appeals. The FOIAXpress system processes FOIA request data received by FOIA users. The Public Access Link component of FOIAXpress enables the public to submit and track the status of FOIA and Privacy Act requests over the internet.

FOIAXpress has been included in this year's representative subset of systems to be evaluated because it is one of the U.S. Office of Personnel Management's (OPM's) moderate risk, major systems, and an audit of its information technology (IT) security controls has not previously been performed.

II. OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The objective of this audit was to determine whether the OPM Office of the Chief Information Officer (OCIO) has implemented IT security controls for FOIAXpress 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 FOIAXpress as of March 2026.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS), issued by the U.S. Comptroller General. GAGAS requires 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 the following security program elements were implemented for FOIAXpress:

- Security Categorization
- Privacy Impact Assessment (PIA)
- System Security and Privacy Plan
- Security and Risk Assessments
- Continuous Monitoring
- Plan of Action and Milestones (POA&M)
- Authorization Memorandum
- Contingency Planning
- 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 FOIAXpress' 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 FOIAXpress' internal control structure in planning our audit procedures. These procedures were mainly substantive in nature; however, we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objective. Because our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on FOIAXpress' internal controls taken as a whole.

The OPM Office of the Inspector General (OIG), as established by the IG Act, performed the audit. The OPM OIG conducted the audit remotely from OPM's Cranberry Township, Pennsylvania and Washington, D.C. offices between August 2025 and March 2026.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting this audit, various laws, regulations, and industry standards were used as criteria to evaluate FOIAXpress' 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 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations;
- NIST SP 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; 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 Recommendations.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. SECURITY CATEGORIZATION

FOIAXpress' security categorization is adequate.

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.

FOIAXpress' 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 FOIAXpress 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 FOIAXpress' overall security categorization as "moderate."

FOIAXpress' security categorization is consistent with FIPS Publication 199 requirements. Additionally, the requirements of NIST SP 800-53, Revision 5, control RA-2 Security Categorization, have been adequately implemented.

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

B. PRIVACY IMPACT ASSESSMENT

FOIAXpress' Privacy Impact Assessment is adequate.

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.

FOIAXpress' PTA was last updated in December of 2024 and concluded that a PIA is required. In accordance with OPM procedures, the PTA's designation was reviewed and reapproved by a designee of OPM's Chief Privacy Officer before the PTA's expiration date. Since FOIAXpress is a privacy sensitive system, the requirements of NIST SP 800-53, Revision 5, control RA-8 Privacy Impact Assessments apply. We reviewed the system's PIA and determined that the

control elements have been adequately implemented. A PIA was provided and last updated on June 26, 2025.

No opportunities for improvement related to FOIAXpress' PIA were identified.

C. SYSTEM SECURITY AND PRIVACY PLAN

OMB Circular A-130 requires that agencies develop and maintain security and privacy plans for all federal information systems. These plans document the security and privacy requirements of a system and describe the controls that are in place or planned to meet those requirements.

FOIAXpress' SPP is current and adequately documented.

For federal information systems to be granted an authorization to operate (ATO), a senior management official must accept the risks associated with the system. The decision to accept those risks should be based on an assessment of all the security controls that are applicable to the system. The SPP establishes and documents security and privacy controls for the system and is the basis for the authorization.

FOIAXpress' SPP satisfies the requirements of NIST SP 800-53, Revision 5, control PL-2 System Security and Privacy Plans, including, but not limited to the following:

- Identifying individuals who fulfill system roles and responsibilities;
- Providing the security categorization and supporting rationale for the system; and
- Describing the mission and business processes supported by the system.

No opportunities for improvement related to FOIAXpress' SPP 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 … ." The authorization to operate the system is based on a determination of the risk to agency operations, assets, individuals, other organizations, and the nation resulting from the operating and use of the system and the decision by the authorization official that this risk is acceptable.

FOIAXpress' security and risk assessments were adequately documented.

According to the OCIO Implementation Procedures and Guidelines: Risk Management Framework, the security assessment plan (SAP) describes a security assessment's scope and

procedures. Using the SAP, an assessment of the system's implemented security controls will be performed. The results of the assessment are recorded in OPM's Governance, Risk, and Compliance (GRC) tool, Archer.

OPM tests the system's applicable controls over a 3-year period. A subset of controls are tested triennially during an independent security controls assessment. The remaining controls are tested as part of the system's continuous monitoring activities.

FOIAXpress' most recent SAP was for an independent security controls assessment performed from April 2022 to May 2022. 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 FOIAXpress' authorizing official (AO).

All requirements of NIST SP 800-53, Revision 5, control CA-2 Control Assessments and RA-3 Risk Assessment have been adequately implemented by FOIAXpress' security and risk assessments.

No opportunities for improvement related to FOIAXpress' 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.

FOIAXpress consistently conducted the necessary ongoing security control assessments.

OPM's Cybersecurity and Privacy Policy requires the OCIO to develop a continuous monitoring strategy and implement a continuous monitoring program.

Our review of OPM's continuous monitoring program demonstrated that the agency is adhering to the following requirements of NIST SP 800-53, Revision 5, control CA-7 Continuous Monitoring:

- Establishing the system-level metrics that must be monitored;
- Establishing organization-defined frequencies for monitoring and for assessment of control effectiveness;

- Correlation and analysis of information generated by control assessments and monitoring; and

- Response actions to address results of the analysis of control assessments.

OPM uses its GRC tool to track continuous monitoring activities. We reviewed FOIAXpress' continuous monitoring assessments between September 2024 and June 2025 to determine whether the security controls were being sufficiently tested per the frequency required by OPM's continuous monitoring program. We determined that continuous monitoring was adequately conducted for the applicable FOIAXpress security controls.

F. PLAN OF ACTION AND MILESTONES

A POA&M is an action plan used by federal agencies to describe steps that will be taken to remediate control weaknesses that are identified during control assessments, audits, and continuous monitoring. POA&Ms define resource requirements, milestones, and timelines.

FOIAXpress' POA&Ms were adequately performed in accordance with policy.

OPM has implemented agencywide POA&M procedures to track known IT security weaknesses associated with the agency's information systems. The AO must consider if the remaining known vulnerabilities in the POA&Ms pose an acceptable level of risk to agency operations, assets, and data. The OCIO Implementation Procedures and Guidelines: Risk Management Framework state that POA&Ms do not have to be remediated prior to authorization. However, the AO may require the remediation of weaknesses prior to authorization. POA&Ms are recorded in OPM's GRC tool, so that risks are continually managed. If POA&M risks cannot be remediated, an acceptance of risk may be completed.

All requirements of NIST SP 800-53, Revision 5, control CA-5 Plan of Action and Milestones have been adequately implemented.

No opportunities for improvement related to FOIAXpress' management of POA&Ms were identified.

G. AUTHORIZATION MEMORANDUM

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

FOIAXpress' ATO memorandum is not signed by the current AO.

FOIAXpress received an ongoing authorization to operate in September 2022. When an ongoing authorization is issued, risks are monitored against OPM's risk tolerance on an ongoing basis. The authorization is

contingent upon continuing to manage risk in accordance with current OPM policies and procedures and fulfilling responsibilities specified in the authorization memorandum.

These responsibilities include the following:

- Continued mitigation and/or remediation of any open POA&Ms 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 FOIAXpress' authorization memorandum also demonstrated that OPM is adhering to the following requirements of NIST SP 800-53, Revision 5, control CA-6, Authorization:

- A senior official had been assigned as the AO for FOIAXpress; and
- The former AO had documented authorization for the system before commencing operations.

However, we identified the following opportunity for improvement related to the ATO memorandum.

1. Change in Authorizing Official

OPM's GRC tool identifies FOIAXpress' current AO. However, the ATO memorandum was signed by the previous AO, who is no longer with the agency. Therefore, FOIAXpress is not compliant with the responsibilities listed in OPM's Cybersecurity and Privacy Policy. This concern is compounded by the fact that the system owner recently left the agency and that several risks were identified and accepted by the previous AO.

NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations states that "When there is a change in authorizing officials, the new authorizing official reviews the current authorization decision document, authorization package, any updated documents from ongoing monitoring activities, or a report from automated security/privacy management and reporting tools. If the new authorizing official finds the current risk to be acceptable, the official signs a new or updated authorization decision document, formally transferring responsibility and accountability for the system or the common controls. In doing so, the new authorizing official explicitly accepts the risk to organizational operations and assets, individuals, other organizations, and the Nation."

OCIO's Implementation Procedures and Guidelines: Risk Management Framework requires that the AO signs an ATO memorandum that formally authorizes the IT system or service for processing.

Without explicit risk acceptance by the newly designated AO, security and privacy risks may persist without informed executive-level acknowledgment, increasing the potential for adverse impacts to mission delivery, system availability, confidentiality, integrity, and stakeholder trust.

Recommendation 1

We recommend that the current authorizing official determine if the risk to organizational operations, organizational data, and assets is acceptable.

OPM Response:

"Concur. OPM has taken action to address this recommendation."

OIG Comment:

As part of the audit resolution process, please provide the OIG with evidence that the recommendation has been fully implemented.

Recommendation 2

We recommend that the current authorizing official issue an authorization decision in the form of an authority to operate memorandum.

OPM Response:

"Concur. OPM has taken action to address this recommendation."

OIG Comment:

As part of the audit resolution process, please provide the OIG with evidence that the recommendation has been fully implemented.

H. CONTINGENCY PLANNING

OMB Circular A-130 requires that federal agencies develop and test contingency plans for all their information systems. Contingency planning refers to policies, procedures, and techniques employed to proactively define and prepare a response to recover information systems in the event of a service impacting incident.

FOIAXpress has an adequate contingency plan.

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 (BIA), which is a key component of the

contingency planning process. 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 documenting both the BIA and the contingency plan to ensure the organization adheres to NIST requirements.

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

FOIAXpress' BIA, contingency plan, and contingency plan testing documentation satisfy the requirements of NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems and NIST SP 800-53, Revision 5, controls CP-2 Contingency Plan and CP-4 Contingency Plan Testing, which include the following:

- 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 FOIAXpress' contingency planning 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.

FOIAXpress adequately implemented all the controls tested.

FOIAXpress is a cloud-based software as a service application that is owned and maintained by a cloud service provider who is solely responsible for implementing 158 out of 197 NIST SP 800-53, Revision 5, controls that are applicable to FOIAXpress. We judgmentally chose to test 23 controls that are classified as hybrid or system specific (i.e., controls in which OPM has a role in implementing). We evaluated these controls by interviewing subject matter experts, reviewing documentation and system screenshots, and viewing a demonstration of system capabilities. One or more controls from each of the following control families were tested:

- Access Control
- Assessment, Authorization, and Monitoring
- Identification and Authentication
- Audit and Accountability
- Contingency Planning
- Planning

- Personally Identifiable Information Processing and Transparency
- Risk Assessment

No opportunities for improvement related to our sample of FOIAXpress' controls were identified.

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the Chief Information Officer

April 15, 2026

MEMORANDUM FOR: Eric Keehan
Deputy Assistant Inspector General for Audits (acting)
Office of the Inspector General

FROM: Adam Starr
Chief Information Officer

SUBJECT: Management's Response to the Final Audit Report 2025-ISAG-024 Audit of the Information Technology Security Controls of OPM's Freedom of Information Act Xpress System

The Office of the Chief Information Officer (CIO) appreciates the opportunity to provide a response to the subject report. The Office of the CIO values open dialogue and partnership with the Office of the Inspector General (OIG) as we safeguard the agency's applications, systems, and data. Our request and responses to the recommendations are below.

Recommendation 1: We recommend that the current authorizing official determine if the risk to organizational operations, organizational data, and assets is acceptable.

Management's Response: Concur. OPM has taken action to address this recommendation.

Recommendation 2: We recommend that the current authorizing official issue an authorization decision in the form of an authority to operate memorandum.

Management's Response: Concur. OPM has taken action to address this recommendation.

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

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