Audit of the EPA's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2025

July 14, 2026 | Report No. 26-P-0041

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

Abbreviations

CIO	Chief Information Officer
DLP	Data Loss Prevention
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GRC	Governance, Risk, and Compliance
IG	Inspector General
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
U.S.C.	United States Code

Cover Image

A laptop showing a red cybersecurity triangle alert icon with "FY25" written underneath. The laptop is in the middle of the image and is surrounded by illuminated locks. (iStock.com/Ruangrit image as modified by the EPA OIG)

Are you aware of fraud, waste, or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, D.C. 20460
(888) 546-8740
OIG.Hotline@epa.gov

Learn more about our OIG Hotline.

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, D.C. 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates.
Follow us on X @EPAoig.
Send us your Project Suggestions.

26-P-0041
July 14, 2026

At a Glance

Audit of the EPA's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2025

Why We Did This Audit

To accomplish this objective:

The U.S. Environmental Protection Agency Office of Inspector General conducted this audit to assess the EPA's compliance with the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*. The Federal Information Security Modernization Act requires the inspector general of each agency to conduct an independent evaluation each year to determine the effectiveness of the agency's information security program and practices.

The reporting metrics outline six security function areas and ten corresponding domains to help federal agencies manage cybersecurity risks. It specifies 20 core and five supplemental metrics across those ten domains, which the agencies' inspectors general are to assess to determine the maturity level of the information security programs. There are five maturity levels, from "ad hoc" (Level 1) to "optimized" (Level 5).

The EPA Cybersecurity, Privacy & Risk Management Division under the Office of the Chief Information Officer, which resides within the EPA Office of Finance and Administration, administers the Agency's information security program.

To support these EPA mission-related efforts:

- *Compliance with the law.*
- *Operating efficiently and effectively.*

Address inquiries to our public affairs office at (202) 566-2391 or OIG.PublicAffairs@epa.gov.

List of OIG reports.

What We Found

We assessed the EPA's information security program against the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*. The Agency achieved Level 4 ratings for 19, or more than three-quarters, of the 25 fiscal year 2025 metrics, and we concluded that the EPA's information security program achieved an overall maturity rating of Level 4. This maturity rating indicates that the program is "managed and measurable," meaning that the EPA collects quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies across the organization and uses those measures to assess and make necessary changes. However, we did identify program deficiencies in the following areas:

- Data loss prevention. The data loss prevention tool that the EPA uses did not block the transmission of data that appeared to be sensitive and confidential, such as social security and credit card numbers, outside of the Agency's network.
- Supply chain risk management controls. The Agency has not updated its system security plans in its governance, risk, and compliance tool, which prevents the EPA from tracking the implementation and effectiveness of the required supply chain risk management controls. Also, the EPA cannot ensure that it has established service level agreements with the third-party vendors that operate, either in whole or part, Agency systems.
- Role-based training compliance. The regional and program offices are not consistently validating their list of personnel with significant information technology security responsibilities nor their personnel's compliance with training requirements. As a result, they are not removing system access from unauthorized users who have significant responsibilities but have not completed the required training.

> **Without effective security controls to mitigate supply chain, data loss prevention, and role-based access vulnerabilities, the Agency risks exfiltration, removal, or modification of its data by malicious internal or external actors.**

Recommendations and Planned Agency Corrective Actions

We make six recommendations to the chief financial officer and chief administrative officer, including to implement data transmission controls and conduct oversight to confirm the data loss prevention tool's effectiveness; develop and implement a plan to update system security plans with supply chain risk controls and verify service level agreements for EPA systems operated by third-party vendors; and develop a process to maintain an accurate list of personnel with significant security responsibilities and periodically validate that they have completed training. The Agency concurred with our recommendations; completed corrective actions for Recommendation 5; and provided acceptable planned corrective actions with estimated milestone dates to address the remaining recommendations, which we consider resolved with corrective actions pending.

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

July 14, 2026

MEMORANDUM

SUBJECT: Audit of the EPA's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2025
Report No. 26-P-0041

FROM: Nicole N. Murley, Deputy Inspector General performing the duties of the Inspector General

TO: C. Paige Hanson, Chief Financial Officer and Chief Administrative Officer
Office of Finance and Administration

This is our report on the subject audit conducted by the U.S. Environmental Protection Agency Office of Inspector General. The project number for this audit was OA-FY25-0041. This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The EPA Office of Finance and Administration is responsible for the issues discussed in this report.

In accordance with EPA Manual 2750, your office completed corrective actions for Recommendation 5 and provided acceptable planned corrective actions and estimated milestone dates in response to the other five recommendations. All six recommendations are therefore either closed or resolved, and no final response to this report is required. If your office submits a response, however, it will be posted on the OIG's website, along with our memorandum commenting on the response. The response should be provided as an Adobe PDF file that complies with the requirements of section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that your office does not want released to the public; if the response contains such data, your office should identify the data for redaction or removal along with corresponding justification.

We will post this report to our website at www.epa.gov/oig.

Table of Contents

Chapters

Appendixes

Chapter 1
Introduction

Purpose

The U.S. Environmental Protection Agency Office of Inspector General initiated this audit to assess the EPA's compliance with the fiscal year 2025 inspector general, or IG, reporting metrics for the Federal Information Security Modernization Act of 2014, or FISMA.

Background

As stewards of the country's information, federal agencies must act to protect our data from cyber threats and malicious actors. Specifically, FISMA mandates that federal agencies provide effective information security, and the National Institute of Standards and Technology, or NIST, provides that agencies should be responsible for "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized activity or system behavior) to provide confidentiality, integrity, and availability."[1] To that end, FISMA at 44 U.S.C. § 3553(a)(2) requires agencies to maintain:

> [I]nformation security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of (A) information collected or maintained by or on behalf of an agency or (B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

Additionally, FISMA requires the IG of each agency to conduct an independent evaluation each year of the agency's information security program and practices to determine their effectiveness. To facilitate these evaluations, the Office of Management and Budget, or OMB, annually issues a document identifying the information security metrics to be assessed that fiscal year. The OMB's *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 2.0, dated April 3, 2025, identifies 20 core and five supplemental FISMA metrics to be assessed. As discussed in the *IG FISMA Reporting Metrics*, core metrics represent a combination of administration priorities and high-value security controls that the IGs must evaluate annually. We list the core metrics for FY 2025 in Appendix A. The supplemental metrics, which the IGs must evaluate once every two years, represent other important activities conducted by information security programs. We list the supplemental metrics for FY 2025 in Appendix B.

Each year, the IGs must report the results of their FISMA evaluations using what is known as the CyberScope template. In this template, the FISMA metrics are posed as questions that address the

[1] NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations (2020).

effectiveness of an information security program. As shown in Table 1, the *IG FISMA Reporting Metrics* addresses six function areas, which are further broken down into ten domains representing the different environments and contexts of an information security program. The six function areas in the *IG FISMA Reporting Metrics* align with those identified in NIST's *Cybersecurity Framework 2.0*, dated February 26, 2024, which also identifies related activities and outcomes for each function area. Individually, the metrics help the IGs to assess the effectiveness of each function area and domain; taken collectively, the metrics present a picture of the health of an agency's information security program. We include the CyberScope template in Appendix C.

Table 1: *IG FISMA Reporting Metrics* and NIST *Cybersecurity Framework* function areas, domains, activities, and outcomes

Function area	Domain	Related activities and outcomes
Govern	Cybersecurity Governance	Organizational context; risk management strategy; roles, responsibilities, and authorities; policy; and oversight
Govern	Cybersecurity Supply Chain Risk Management	Cybersecurity supply chain risk management
Identify	Risk and Asset Management	Asset management, risk assessment, and risk management strategy
Protect	Configuration Management	Technology infrastructure resilience
Protect	Identity and Access Management	Identity management, authentication, and access control
Protect	Data Protection and Privacy	Data security and platform security
Protect	Security Training	Awareness and training
Detect	Information Security Continuous Monitoring	Continuous monitoring and adverse event analysis
Respond	Incident Response	Incident management, incident analysis, incident response reporting and communication, and incident mitigation
Recover	Contingency Planning	Incident recovery plan execution and incident recovery communication

Source: The OMB's *IG FISMA Reporting Metrics* and NIST's *Cybersecurity Framework 2.0*. (EPA OIG table)

The IGs assess the effectiveness of each function area and domain, as well as the information security program as a whole, on a maturity model spectrum with five levels. As shown in Figure 1, a rating at the foundational levels of this spectrum signifies that an agency has developed some measure of policies and procedures, while a rating at the advanced levels captures the extent to which an agency has institutionalized those policies and procedures. Within the context of the maturity model, the *IG FISMA Reporting Metrics* states that the OMB believes a Level 4 rating or above represents an effective level of security. A metric or program that receives a Level 4 rating is one for which the organization collects quantitative and qualitative measures on the effectiveness of the applicable policies, procedures, and strategies and uses those measures to assess and make necessary changes to the policies, procedures, and strategies.

Figure 1: Maturity model spectrum

Source: The OMB's *IG FISMA Reporting Metrics*. (EPA OIG image)

Data privacy and protection is a critical component of information security. NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* updated December 2020, provides that agencies need to protect the confidentiality and integrity of data in transit within and outside of their networks, as well as the confidentiality and integrity of any system component that can transmit data. Additionally, NIST states that agencies need to protect their data that are not in transit, which we refer to in this report as data at rest. Pursuant to 42 U.S.C. § 2000ee-2, which requires agencies to have privacy and data protection policies in place, IGs must conduct a periodic review of their respective agency's implementation of those policies. Although this periodic review is separate from the annual FISMA evaluation, IGs may include the results of this review as part of their FISMA reporting.

Data at rest and in transit

As the terms suggest, "data at rest" is information not in process or in transit that is located on system components, while "data in transit" is information moving between system components.

To protect data in transit, the EPA uses a data loss prevention tool, which is owned and operated by a third-party vendor. The tool's data transmission controls can be customized to detect and prevent certain information from being sent between systems both internal and external to the Agency, such as by email. To protect data at rest, the EPA uses a variety of internal controls, such as encryption and exfiltration controls. Exfiltration controls are security measures that prevent the theft or unauthorized removal or movement of data from a device.

Responsible Offices

According to the EPA's website, the EPA Office of Finance and Administration leads Agency core mission support functions, such as protection of the EPA's facilities and critical assets nationwide.[2] This office also provides critical resources, tools, solutions, and support services related to information technology and its management that enable the EPA to protect human health and the environment.

The EPA's chief information security officer resides within the Office of Finance and Administration's Office of the Chief Information Officer. This office includes the Cybersecurity, Privacy & Risk Management Division, which promotes agencywide cooperation in managing risks and protecting EPA information and defines clear, comprehensive, and enterprisewide information security and privacy strategies. In FY 2025, the EPA allocated $8,388,000 to its information security efforts.[3]

Scope and Methodology

We conducted this performance audit from March 2025 to March 2026 in accordance with generally accepted government auditing standards. Those 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We assessed the internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed control environment, risk assessment, control activities, information and communication, and monitoring controls significant to our audit objective. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

We assessed the EPA's compliance with the 20 core and five supplemental FISMA metrics required for FY 2025. We assessed these 25 metrics up to Maturity Level 4, "managed and measurable." In other words, the highest maturity level that we tested for and rated was Level 4, which the OMB believes is an effective level of security. For those metrics that did not result in a maturity rating of Level 4, we documented justifications for those ratings. We provide an overview of our FISMA audit results in Chapter 2 and Appendix D.

[2] Prior to November 16, 2025, the EPA Office of Mission Support was responsible for the topics discussed in this report. On that date, the EPA merged that office and the EPA Office of the Chief Financial Officer to establish the Office of Finance and Administration. Although the scope of our audit was FY 2025, which ended before the reorganization, we refer to the Office of Finance and Administration as the responsible office, since the head of that office, the chief financial officer and chief administrative officer, is the action officer for the recommendations resulting from this audit.

[3] In FY 2025, the funds for information security were allocated to the former Information Technology Security and Privacy Program, which was located within the former Office of Mission Support's Office of Information Security and Privacy.

We interviewed Agency personnel, inspected relevant Agency information technology documentation, and analyzed evidence supporting the EPA's compliance with the metrics outlined in the *IG FISMA Reporting Metrics*. We also selected the EPA's Enterprise Wide Area Network, a system containing personally identifiable information that provides internal and external connectivity for the Agency, as the sample system for assessing controls for the FISMA metrics targeted at the system level. On July 1, 2025, we provided the Agency with our assessment and discussed the results. On July 29, 2025, we submitted the required CyberScope template, which includes our assessment for each of the 25 FY 2025 FISMA metrics, as required by the OMB. We include our completed CyberScope template in Appendix C.

For FY 2025, we also reviewed the Agency's implementation of data protection and privacy procedures, as required by 42 U.S.C. § 2000ee-2. We assessed data in transit between internal and external systems, as well as data at rest on an Agency system. To assess the EPA's controls to protect its data in transit, we conducted live testing of the Agency's data loss prevention, or DLP, tool. With advance notice to and in the presence of EPA personnel, we sent four emails containing fabricated sensitive and confidential information, including fabricated personally identifiable information, from an EPA email address to a nongovernment email address to determine whether the DLP tool could prevent the unauthorized disclosure of such information. To assess the EPA's controls to protect its data at rest, we reviewed configuration settings for drive encryption, password encryption, and Universal Serial Bus data exfiltration controls on the Enterprise Wide Area Network's access control servers, where sensitive and confidential information resides.[4] We documented our assessment as part of the CyberScope template's FISMA metric 23.2 within the Data Protection and Privacy domain. We provide additional details in Chapter 2 of this report.

Prior Reports

In EPA OIG Report No. 25-P-0023, *Audit of the EPA's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2024*, issued April 2, 2025, we recommended that the Agency develop and implement procedures for validating systems inventory data received by the regional and program office senior information officers; develop and implement procedures to reconcile software purchase data in the software asset management tool with software installations; and document the software asset management tool's designation as the system of record for the Agency's enterprise software asset management, as well as instruct senior information officials and relevant information technology personnel of that designation. As of July 2025, these recommendations were resolved with corrective actions pending.

For this current audit, we followed up on the recommendations from EPA OIG Report No. 24-P-0052, *The EPA Needs to Develop and Implement Information Technology Processes to Comply with the Federal Information Security Modernization Act for Fiscal Year 2023*, issued August 5, 2024. In that prior report, we recommended that the Agency develop and implement an automated process for detecting unauthorized hardware on the EPA network, collaborate with system owners and other relevant

[4] Universal Serial Bus is the system for connecting electronic equipment to devices like computers and moving data between them.

information technology personnel to conduct a root-cause analysis of common baseline configuration compliance findings to determine the source of these issues from an enterprise level, and complete the Agency's plan to fulfill Event Logging Tier 1 and Event Logging Tier 2 maturity requirements on the EPA network. During this current audit, we confirmed that all corrective actions have been completed.

We also followed up on the recommendations from EPA OIG Report No. 23-E-0021, *The EPA's Vulnerability Tracking and Remediation and Information Technology Procedures Review Processes Are Implemented Inconsistently*, issued July 5, 2023. That prior report stated that the Agency did not update its information security procedures to incorporate controls outlined in NIST Special Publication 800-53, Revision 5, within one year of its publication date, as required by OMB Circular No. A-130, *Managing Information as a Strategic Resource*, dated July 28, 2016. In that report, we recommended that the EPA update CIO 2190.0-P-01.0, *Reviewing and Updating Agencywide Directives Administered by the EPA CIO*, to include a timely process for reviewing and updating information security procedures within a year of the issuance of relevant NIST publications. During this current audit, we confirmed that the EPA completed the corrective action on December 1, 2023.

Chapter 2
The EPA's Information Security Program Receives Level 4 Maturity Rating, but Several Deficiencies Exist, Including Ineffective Data Loss Prevention Controls

Overall, we assessed the Agency's information security program at the Level 4 maturity rating of "managed and measurable," as shown in Appendix D. Only six of the 25 metrics that we assessed for FY 2025 received a rating lower than Level 4. We previously identified three of these deficiencies in our FY 2024 FISMA report, and the EPA has corrective actions underway.[5] As reflected in our completed CyberScope template in Appendix C, the three other areas of deficiency that we identified fall within the following two function areas and three domains:

- Protect function area, Data Protection and Privacy domain, FISMA metric 23.2. Although we ultimately assessed this metric to be at the Level 4 maturity rating, we reported the results of our "periodic review" of the Agency's data protection and privacy procedures pursuant to 42 U.S.C. § 2000ee-2 under this metric. We detail the results of our review in this chapter.
- Govern function area, Cybersecurity Supply Chain Risk Management domain, FISMA metric 5. We assessed this metric at the Level 3 maturity rating of "consistently implemented." We detail this finding in Chapter 3.
- Protect function area, Security Training domain, FISMA metrics 24 and 25.1. We assessed these two metrics at the Level 3 maturity rating. We detail this finding in Chapter 4.

When we reviewed the Agency's data protection and privacy procedures pursuant to 42 U.S.C. § 2000ee-2, we found that the EPA's controls to protect data at rest on its Enterprise Wide Area Network are operating effectively. However, the EPA's controls to protect data in transit from its internal systems to external systems are not operating effectively. Specifically, the EPA's DLP tool, which is owned and operated by a third-party vendor, was unable to always block the transmission of sensitive and confidential information to an outside, nongovernmental email address.[6] Of the four test emails that we sent, the DLP tool failed to prevent three from leaving the EPA network. This occurred because the DLP tool lacks customization that would provide for effective data transmission controls. Also, the Agency does not conduct regular oversight of the DLP tool. Without effective controls to prevent the transmission of sensitive and confidential information, the EPA risks unauthorized disclosure of this type of information, including the personally identifiable information of

[5] As noted in the "Prior Reports" section in Chapter 1, we issued three recommendations in EPA OIG Report No. 25-P-0023, *Audit of the EPA's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2024*, dated April 2, 2025.

[6] As noted in the "Scope and Methodology" section in Chapter 1, we sent four emails with fabricated personally identifiable information from an EPA email to a nongovernmental email to test whether the DLP tool would block the transmission of such information to an outside system.

its stakeholders and employees. Such disclosures put the information at risk of use or modification by malicious actors, increasing the likelihood of identity fraud and eroding the public's trust in the EPA's ability to protect its information.

The Data Loss Prevention Tool Needs to Be Updated to Block the External Transmission of Sensitive and Confidential Information

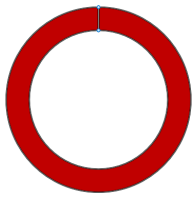
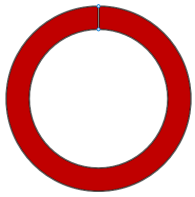
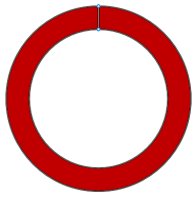
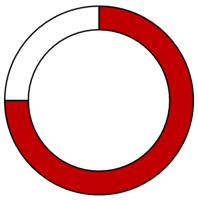
We identified gaps in the DLP tool's data transmission controls to protect data in transit. Of the four test emails that we sent with sensitive and confidential data, the DLP tool successfully blocked only one. This means that the sensitive and confidential information in the other three emails, albeit fabricated for testing purposes, was disclosed outside of the Agency's network. Among the types of sensitive and confidential information included in these emails were full names, telephone numbers, personal identification numbers, credit card verification values, and international bank account numbers. Table 2 illustrates the results of our four test emails and the types of sensitive data contained in those emails. It is important to note that our first test email, which was blocked, contained overtly fabricated information such as all 1's for a social security or credit card number. Our fourth test email included some of that same information—but as an attachment instead of in the body of the email. As indicated previously, the DLP tool failed to block the transmission of that fourth email.[7]

The EPA's failure to protect the confidentiality and integrity of data in transit is contrary to NIST requirements in Special Publication 800-53, specifically control SC-8, "Transmission Confidentiality and Integrity." Furthermore, the EPA is not complying with its Directive No. CIO 2150.3-P-16.2, *Information Security–System and Communications Protection (SC) Procedure*, dated November 21, 2023, which requires the implementation of NIST Special Publication 800-53 controls for all EPA information and information systems related to the system and communications protection control family.

Table 2: Results of DLP tool testing

Email test	Transmitted data elements	Transmission blocked by DLP tool?	Percent of failure (%)
1	Transmitted in the body of the email: • First and last name. • International bank account number. • Permanent account number.* • Card verification value. • Personal identification number. • Social security number. • Credit card number.	Yes ☑	0

[7] EPA Directive No. 2151-P-10.0, *Protecting Sensitive Personally Identifiable Information (SPII)*, dated December 19, 2016, states that employees must "[n]ever send unencrypted email containing SPII [sensitive personally identifiable information]." However, the DLP tool should be able to detect and prevent unencrypted transmissions in the event that proper encryption controls are not used. Our tests did not use encryption.

Email test	Transmitted data elements	Transmission blocked by DLP tool?	Percent of failure (%)
2	Transmitted in the body of the email: • First and last name. • Phone number. • International bank account number. • Permanent account number. • Card verification value. • Personal identification number.	No ☒	100 
3	Transmitted in the body of the email: • First and last name. • Phone number. • International bank account number. • Permanent account number. • Card verification value. • Personal identification number.	No ☒	100 
4	Transmitted via a document attachment: • First and last name. • Social security number. • Credit card number.	No ☒	100 
TOTAL	—	—	**75** 

Source: OIG testing data. (EPA OIG table)

* A permanent account number is a ten-digit unique alphanumeric number issued by the Government of India's Income Tax Department that enables the department to link all transactions conducted by the number holder with the department.

Agency personnel stated that, with the exception of the first email test that contained overtly fabricated information, the DLP tool failed to block our emails because it had not been customized to identify and block the information tested. These missing data transmission controls allowed what appeared to be sensitive and confidential information to be transmitted from the EPA's systems to an external system. Agency personnel also said that information like international bank account and permanent account numbers follow international standards, while the DLP tool is built on U.S. standards. However, the EPA's "Partnering with International Organizations" web page, updated on January 23, 2026, states that the Agency collaborates with multilateral organizations and foreign partners to encourage "collective actions for common solutions and help leverage resources … to manage ongoing and emerging environmental threats." The EPA's bilateral cooperative programs operate in Antarctica, Asia, Europe, Latin America, the Middle East, and Africa, so a focus on U.S. standards for data protection is not

adequate. Additionally, the DLP tool vendor said that relevant keywords, such as "credit card" or "SSN," must be included within the email's text for the tool to detect and block the number pattern from transmission. Such keywords, however, may not always be present in emails.

Beyond the DLP tool's missing and ineffective data transmission controls, the Agency does not conduct regular oversight of the tool or the vendor's customization of the tool. Instead, the Agency is trusting that the third-party tool's continuous real-time protection identifies all transmitted sensitive and personally identifiable information and operates as needed. Without regular oversight of the DLP tool, the Agency is not ensuring that the DLP tool is operating effectively throughout the year.

Without effective DLP tool data transmission controls, the Agency risks the exfiltration of personally identifiable and other sensitive and confidential information when data is in transit. Information that is being transmitted via unprotected communication paths like emails not only may be intercepted but also may be modified. As a result, EPA stakeholders, including the Agency's employees, its regulated industries, and anyone who communicates with the Agency, may be at increased risk of identity fraud. Furthermore, the public's trust in the EPA's ability to protect its information may be irreparably eroded.

Recommendations

We recommend that the chief financial officer and chief administrative officer:

1. Implement controls to prevent and detect the transmission of all sensitive and confidential information by the data loss prevention tool. This effort would help correct data loss prevention gaps that allow the transmission of sensitive and confidential information outside the Agency's network.

2. Develop and implement controls to periodically confirm the operational effectiveness of the data loss prevention tool's data transmission controls. This process would improve Agency oversight of the data loss prevention tool's data transmission controls.

Agency Response and OIG Assessment

The EPA concurred with our recommendations and provided acceptable planned corrective actions and estimated milestone dates. We include the Agency's response to our draft report in Appendix E.

Regarding Recommendation 1, the EPA concurred that it lacks controls to prevent and detect transmission of sensitive data outside of its network. Similarly for Recommendation 2, the Agency concurred with the need to periodically confirm operational effectiveness of the DLP tool. We believe that the proposed corrective actions will satisfy the intent of these recommendations, which we consider resolved with corrective actions pending.

Chapter 3
The EPA Needs to Track Implementation of Supply Chain Risk Management Requirements for Its Systems

We assessed the EPA's Cybersecurity Supply Chain Risk Management domain to be at the Level 3 maturity rating of "consistently implemented." The Agency's governance, risk, and compliance, or GRC, tool, which is a software application operated by a third-party vendor, does not fully incorporate NIST requirements for managing cybersecurity risks within and across its supply chains—the external third-party vendors that the Agency works with. While the GRC tool vendor updated the application in March 2025 to reflect the required NIST supply chain risk management security controls, the EPA had not, as of July 2025, completed updating the system security plans maintained within the GRC tool.[8] Without updated system security plans, the Agency cannot track which supply chain risk management security controls need to be implemented and on which information systems they need to be implemented, nor can the Agency assess the effectiveness of any control that was implemented. Consequently, the EPA is at increased risk of data breaches, operational disruption, or other supply chain vulnerabilities.

Governance, risk, and compliance tool

A GRC tool helps organizations manage risks and streamline cybersecurity compliance activities, consistent with NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*. The EPA's Information Security Task Force mandated the use of a GRC tool, which allows users to manage artifacts and documents related to system authorization; enables control inheritance; establishes and manages plans of action and milestones; and generates the system security plans, reports, and documentation needed for security authorization processes and to support the EPA's Risk Management Program.

System security plan

A system security plan is a formal document that provides an overview of the security requirements for an information system and describes the security controls for meeting those requirements.

The EPA Needs to Update Its System Security Plans to Track the Implementation of Supply Chain Risk Management Security Controls

The EPA uses its GRC tool to create and maintain its system security plans, which include the operating status of all planned, implemented, and inherited security controls. OMB Circular No. A-130, *Managing Information as a Strategic Resource*, requires agencies to comply with new or updated NIST standards and guidelines within a year of their publication. Similarly, EPA Directive No. OMS-2023-0001, *Policy for Creating and Maintaining Internal EPA Mission Support Policy,* dated October 17, 2023, provides that "[a]ll Information Security related Policy requires reviews and updates within a year of issuance of

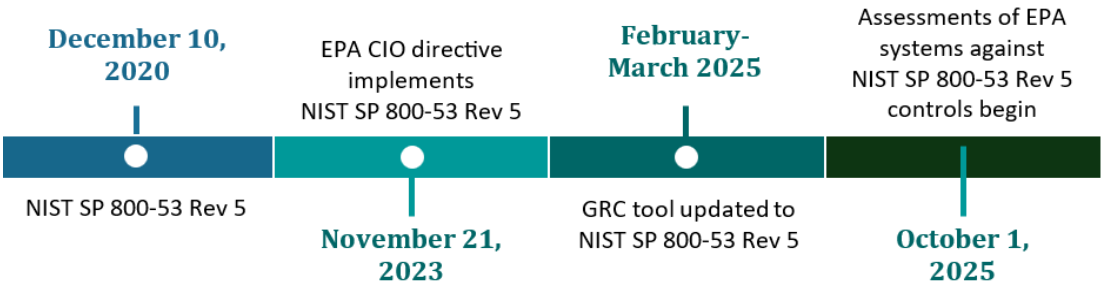
[8] As reported in the "Scope and Methodology" section in Chapter 1, during July 2025 we briefed the Agency on our FISMA audit findings and submitted the CyberScope template to the OMB, which essentially marked the end of our fieldwork.

relevant National Institute of Standards and Technology (NIST) publications." In other words, when a new NIST standard or guideline is published, the EPA must ensure that the GRC tool, including the system security plans maintained in the tool, is updated to incorporate that new standard or guideline within one year.

The EPA requires compliance with NIST standards and guidelines through directives issued by the EPA chief information officer. When NIST publishes a revision of Special Publication 800-53 that includes new security control requirements, the chief information officer issues a directive outlining how the Agency is to incorporate the new controls. The GRC tool itself is updated accordingly, and the EPA's system owners subsequently update their system security plans to document any new controls. Then, in accordance with EPA Directive No. CIO 2150-P-04.3, *Information Security–Assessment, Authorization and Monitoring (CA) Procedure*, dated June 08, 2023, system owners assess and document their assessment of these security controls, either as part of annual security control assessments or following significant changes to the systems or their environment.

Issued in September 2020 and updated in December 2020, Revision 5 of NIST Special Publication 800-53 provides "a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets" from risks like hostile attacks, human error, and privacy breaches. In the Revision 5 catalog was a new family of controls not included in Revision 4: supply chain risk management controls. To comply with OMB Circular No. A-130 and EPA Directive No. OMS-2023-0001, the GRC tool and the Agency's system security plans should have been updated to incorporate these supply chain management controls no later than December 2021—one year after the Revision 5 update. However, as shown in Figure 2, it was not until November 21, 2023, that the EPA chief information officer issued the directive requiring implementation of the Revision 5 controls: Directive No. CIO 2150-P-26.0, *Supply Chain Risk Management (SR) Procedure*. By March 2025, the GRC tool vendor updated the application to reflect the Revision 5 controls. However, as of July 2025, the EPA had still not updated all of its system security plans. Agency personnel told us that each information system owner would document implementation and begin assessment of applicable supply chain risk management security controls in the system security plans by October 1, 2025.[9]

Figure 2: Timeline to align EPA systems with federal and Agency guidance



Source: OIG analysis of federal and Agency guidance. (EPA OIG image)

Notes: CIO = Chief Information Officer; Rev = Revision; SP = Special Publication.

[9] We did not assess whether the EPA accomplished the system security plan updates by this date, as this was outside of the scope of our audit.

As a result of the delayed updates to both the GRC tool and the system security plans, the Agency has also been delayed in implementing and then assessing the operational effectiveness of the supply chain risk management controls, as required by CIO 2150-P-04.3. The Agency said that, once all required updates are made, it would begin assessing the supply chain risk management security controls as part of the systems' annual security control assessments, consistent with CIO 2150-P-04.3. These assessments help the EPA to manage risks, streamline cybersecurity compliance activities, and maintain compliance with updated standards and controls. For example, because establishing service level agreements is one of the required NIST Revision 5 controls for external system services, the assessments will provide the EPA with an opportunity to verify that it has established effective service level agreements with its supply chain vendors. Without effective service level agreements that incorporate the NIST Revision 5 controls, the Agency cannot hold third parties that are operating all or part of a system on the EPA's behalf responsible for meeting the required and agreed-upon standards of service.

Service level agreement

A service level agreement is a documented agreement between a vendor and a customer, such as the EPA, that outlines the service expected, performance metrics, responsibilities, and remedies for failure to meet agreed-upon standards. It is a contract that defines what quality of service a customer should receive and how it will be measured. A service level agreement is crucial for establishing clear expectations, ensuring accountability, and promoting trust between a vendor and the customer.

As part of our FISMA audit, we specifically assessed the supply chain risk management security controls for three EPA systems operated or partially operated by third-party vendors. The Agency had not updated its system security plans in the GRC tool for these three systems to comply with the latest NIST Revision 5 controls, which added the supply chain risk management family of controls. It therefore could not track the supply chain risk management controls for those three systems. It also could not conduct any assessment of supply chain risk management controls to ensure their effective operations. According to Agency personnel, this lack of tracking and assessment encompasses service level agreements. These personnel told us that only when the Revision 5 updates are incorporated into the system security plans will the Agency begin tracking and assessing service level agreements as part of the annual security control assessments.

Beyond the delayed updates to the GRC tool and the system security plans, the Agency said that the delay in implementing, tracking, and assessing the supply chain risk management controls partly occurred because updating system security plans is a laborious process, requiring the EPA to work with the GRC tool vendor to map each EPA system, one at a time, from Revision 4 to Revision 5 controls. Additionally, before that mapping could occur, the Agency had to migrate the GRC tool data to a cloud environment as part of an agencywide cloud migration initiative. Now that the migration and GRC tool updates are completed, the EPA said that it can turn to updating the system security plans with Revision 5 controls, tracking the controls, and assessing their operational effectiveness.

Implementing robust security controls to manage supply chain risks is essential to protecting the integrity, confidentiality, and availability of supply chain operations. By not implementing supply chain

risk management security controls within EPA systems, not tracking these controls, and not consistently assessing these controls, the EPA is at risk of data breaches, operational disruption, or supply chain vulnerabilities. Additionally, by not tracking and assessing service level agreements in particular, the Agency cannot ensure that its third-party vendors are providing effective levels of service.

Recommendations

We recommend that the chief financial officer and chief administrative officer:

3. Develop and implement a plan to complete updates of the EPA's system security plans to incorporate supply chain risk management security controls and requirements that align with National Institute of Standards and Technology Special Publication 800-53, Revision 5. These updates will establish supply chain risk management controls for each EPA system and allow the Agency to track and assess those controls to ensure operational effectiveness.

4. Develop and implement controls to verify that service level agreements are established for EPA systems operated, in whole or part, by third-party vendors, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 5. This will ensure that the vendors are adhering to National Institute of Standards and Technology controls to ensure the operational effectiveness of EPA systems.

Agency Response and OIG Assessment

For Recommendations 3 and 4, the EPA concurred that it lacks system security plans updated with supply chain risk management security controls and requirements, including those related to service level agreements, to align with NIST Special Publication 800-53. We believe that the proposed corrective actions will satisfy the intent of these recommendations, which we consider resolved with corrective actions pending.

Chapter 4
The EPA Needs to Strengthen Its Validation Processes for Role-Based Training Requirements

We assessed the EPA's Security Training domain to be at the Level 3 maturity rating of "consistently implemented." Federal and Agency requirements provide that personnel with cybersecurity and cyberoperations roles must complete role-based training before gaining access to systems and annually thereafter to maintain network access. However, we found that personnel with significant information technology security responsibilities maintained network access even if they did not comply with role-based training requirements. This deficiency occurred because regional and program offices did not consistently validate their list of staff with significant information technology security responsibilities, nor did they ensure that these staff completed the required training to maintain access authorization. If the EPA allows unauthorized users to remain on the Agency's network, there is an increased likelihood of security breaches, data corruption, and compliance violations.

The EPA Needs to Consistently Implement Controls Related to Information Technology Security Personnel and Their Training

The EPA lacks controls to ensure that it identifies all personnel with significant information technology security responsibilities and that those personnel have fulfilled their training requirements. As part of our FISMA assessment, we identified two employees—out of a subset of 31 employees assigned as system administrators—who were noncompliant with role-based security training requirements in FY 2024, the last full training cycle at the time we completed our FISMA audit fieldwork in July 2025.

There are multiple federal and Agency documents that outline role-based security training requirements:

- OMB Circular No. A-130, Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources*, dated July 28, 2016, requires the Agency to provide role-based security training to employees and contractors with assigned security and privacy roles and responsibilities before they are authorized to access systems.
- EPA Directive No. CIO-2150.3-P-19.2, *Information Security–Roles and Responsibilities Procedures*, dated May 19, 2022, states that the chief information security officer and other senior personnel ensure that employees with significant information technology security responsibilities complete role-based information security training and education. Employees with significant information technology security responsibilities would include system owners, system administrators, and information security officers.
- The EPA's *Cybersecurity and Privacy Awareness and Training Plan,* dated March 1, 2024, states that system administrators, among others, are required to take five hours of role-based training on an annual basis. It also states that application owners, among others, are required to take

two hours of role-based training. Senior information officers are to provide a list of staff who do not comply to the appropriate office to disable their accounts.[10]

- EPA Directive No. CIO 2150-P-02.3, *Information Security–Awareness Training (AT) Procedure*, dated June 12, 2023, requires personnel with information technology security responsibilities to complete role-based training before receiving authorized access and annually thereafter.

These deficiencies occurred because senior information officers for some regional and program offices did not consistently validate their list of staff with significant information technology security responsibilities, nor did they validate whether those staff completed the required training. One senior information officer was unaware of a system administrator's categorization as having significant information technology security responsibilities. In addition, we were told that one of the noncompliant system administrators did not complete the training requirements because of an extended leave of absence. Senior information officers did not revoke access despite the system administrator's extended absence and inability to complete the training as required.

While most of the employees whose training documentation we reviewed completed role-based security training requirements in FY 2024, there were still instances of noncompliance, and two employees maintained system access when they should not have. Inconsistent tracking of role-based training compliance weakens the Agency's ability to ensure that only authorized personnel have network access, which in turn weakens the Agency's ability to safeguard the confidentiality, integrity, and availability of the EPA's information and information systems. Unauthorized access to the Agency's network increases the likelihood of security breaches, data corruption, and compliance violations.

Recommendations

We recommend that the chief financial officer and chief administrative officer:

5. Annually instruct senior information officers or similar personnel in charge of employees to maintain a list identifying all their personnel with significant information technology security responsibilities, to certify the completeness and accuracy of this list, and to make these personnel aware of their role-based training requirements. This would improve Agency oversight by ensuring that only authorized personnel have access rights to EPA networks and systems.

6. Develop and implement a process for senior information officers to periodically validate that their personnel with significant information technology security responsibilities have completed the required role-based training. This process would improve the Agency's ability to prevent unauthorized access to the EPA network and safeguard its information and information systems.

[10] Prior to November 2025, the appropriate office was the former Office of Information Security and Privacy within the former Office of Mission Support.

Agency Response and OIG Assessment

The Agency concurred with Recommendations 5 and 6 related to the Agency's process for tracking and validating that personnel with significant information technology security responsibilities have completed the required role-based training. On May 6, 2026, in fulfillment of Recommendation 5, the EPA chief information security officer instructed senior information officers and similar information technology personnel in charge of employees to maintain a list identifying all their personnel with significant information technology security responsibilities, to certify the completeness and accuracy of this list, and to make these personnel aware of their role-based training requirements. Recommendation 5 is therefore closed with corrective action completed.

Additionally, the Agency provided acceptable planned corrective action and an estimated milestone date for Recommendation 6. The corrective action consists of implementing a process for senior information officers to periodically validate that their personnel with significant information technology security responsibilities have completed the required role-based training. We consider Recommendation 6 resolved with corrective action pending.

Status of Recommendations

Rec. No.	Page No.	Recommendation	Status*	Action Official	Planned Completion Date
1	10	Implement controls to prevent and detect the transmission of all sensitive and confidential information by the data loss prevention tool. This effort would help correct data loss prevention gaps that allow the transmission of sensitive and confidential information outside the Agency's network.	R†	Chief Financial Officer and Chief Administrative Officer	5/30/26
2	10	Develop and implement controls to periodically confirm the operational effectiveness of the data loss prevention tool's data transmission controls. This process would improve Agency oversight of the data loss prevention tool's data transmission controls.	R	Chief Financial Officer and Chief Administrative Officer	7/17/26
3	14	Develop and implement a plan to complete updates of the EPA's system security plans to incorporate supply chain risk management security controls and requirements that align with National Institute of Standards and Technology Special Publication 800-53, Revision 5. These updates will establish supply chain risk management controls for each EPA system and allow the Agency to track and assess those controls to ensure operational effectiveness.	R	Chief Financial Officer and Chief Administrative Officer	10/1/26
4	14	Develop and implement controls to verify that service level agreements are established for EPA systems operated, in whole or part, by third-party vendors, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 5. This will ensure that the vendors are adhering to National Institute of Standards and Technology controls to ensure the operational effectiveness of EPA systems.	R	Chief Financial Officer and Chief Administrative Officer	10/30/26
5	16	Annually instruct senior information officers or similar personnel in charge of employees to maintain a list identifying all their personnel with significant information technology security responsibilities, to certify the completeness and accuracy of this list, and to make these personnel aware of their role-based training requirements. This would improve Agency oversight by ensuring that only authorized personnel have access rights to EPA networks and systems.	C	Chief Financial Officer and Chief Administrative Officer	5/6/26
6	16	Develop and implement a process for senior information officers to periodically validate that their personnel with significant information technology security responsibilities have completed the required role-based training. This process would improve the Agency's ability to prevent unauthorized access to the EPA network and safeguard its information and information systems.	R	Chief Financial Officer and Chief Administrative Officer	10/30/26

* C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

† Although the planned completion date for this recommendation is before the report issuance date, we did not change the status to "C" because we did not verify that the EPA completed the corrective action. We will assess recommendation status during our next FISMA audit.

Appendix A

FY 2025 Core IG FISMA Reporting Metrics

The numbers in this table correlate to the metrics in the *IG FISMA Reporting Metrics*. This table lists only the 20 core metrics that the IGs were required to assess for FY 2025. See Appendix C for more details.

Function area	Domain	Metric number	Metric
Govern	Cybersecurity Supply Chain Risk Management	5	To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?
Identify	Risk and Asset Management	7	To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems) and system interconnections?
Identify	Risk and Asset Management	8	To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including Government Furnished Equipment (GFE), Internet of Things [IoT], and Bring Your Own Device [BYOD] mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?
Identify	Risk and Asset Management	9	To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?
Identify	Risk and Asset Management	11	To what extent does the organization ensure that information system security risks are adequately managed?
Identify	Risk and Asset Management	12	To what extent does the organization use technology/automation to provide a centralized, enterprisewide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?
Protect	Configuration Management	14	To what extent does the organization use configuration settings/common secure configurations for its information systems?
Protect	Configuration Management	15	To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP [Internet Protocol] assets?

Function area	Domain	Metric number	Metric
Protect	Identity and Access Management	17	To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV [personal identity verification], FIDO2 [Fast IDentity Online], or web authentication) for non-privileged users to access the organization's physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access?
Protect	Identity and Access Management	18	To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for privileged users to access the organization's physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access?
Protect	Identity and Access Management	19	To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed?
Protect	Data Protection & Privacy	21	To what extent has the organization implemented the following security controls to protect the confidentiality, integrity, and availability of its PII [personally identifiable information] and other agency sensitive data, as appropriate, throughout the data lifecycle? • Encryption of data at rest • Encryption of data in transit • Limitation of transfer to removable media • Sanitization of digital media prior to disposal or reuse • Backups of data are created, protected, maintained, and tested • Access to personal email, external file sharing and storage sites, and personal communication applications are blocked, as appropriate.
Protect	Data Protection & Privacy	22	To what extent has the organization implemented security controls (e.g., DLP, IDPS [intrusion detection and prevention system], CASB [cloud access security broker], User and Entity Behavior Analytic tools, SIEM [security information and event management] and EDR [endpoint detection and response]) to prevent data exfiltration and enhance network defenses?
Protect	Security Training	24	To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide specialized security training within the functional areas of: govern, identify, protect, detect, respond, and recover?

Function area	Domain	Metric number	Metric
Detect	Information Security Continuous Monitoring	26	To what extent does the organization use information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?
Detect	Information Security Continuous Monitoring	28	To what extent does the organization perform ongoing (continuous monitoring) information system assessments to grant system authorizations, including developing and maintaining system security plans, and monitoring system security controls?
Respond	Incident Response	30	To what extent has the organization implemented processes related to incident detection and analysis?
Respond	Incident Response	31	To what extent has the organization implemented processes related to incident handling?
Recover	Contingency Planning	33	To what extent does the organization ensure that the results of BIAs [business impact analysis] are used to guide contingency planning efforts?
Recover	Contingency Planning	34	To what extent does the organization perform tests/exercises of its information system contingency planning processes?

Source: The OMB's *IG FISMA Reporting Metrics*. (EPA OIG table)

FY 2025 Supplemental IG FISMA Reporting Metrics

The numbers in this table correlate to the metrics in the *IG FISMA Reporting Metrics*. The table lists only the five supplemental metrics that the IGs were required to assess for FY 2025. See Appendix C for more details.

Function area	Domain	Metric number	Metric
Govern	Cybersecurity Governance	1	To what extent does the organization develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize and communicate its cybersecurity objectives?
Govern	Cybersecurity Governance	2	To what extent does the organization use a cybersecurity risk management strategy to support operational risk decisions?
Govern	Cybersecurity Governance	3	To what extent do cybersecurity roles, responsibilities, and authorities foster accountability, performance assessment, and continuous improvement?
Identify	Risk and Asset Management	10	To what extent does the organization develop and maintain inventories of data and corresponding metadata for designated data types, as appropriate throughout the data lifecycle?
Detect	Information Security Continuous Monitoring	27	To what extent does the organization monitor and measure the integrity and security posture of all owned and associated assets?

Source: The OMB's *IG FISMA Reporting Metrics*. (EPA OIG table)

OIG-Completed CyberScope Template

Inspector General Section Report	2025 FISMA Annual IG

Environmental Protection Agency

Function 0: Overall

0.1 Please provide an overall IG self-assessment rating (Effective/Not Effective)

Effective

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

The U.S. Environmental Protection Agency Office of Inspector General determined that, overall, the EPA has demonstrated that it effectively implements managed and measurable policies, procedures, and strategies for all six information security function areas in adherence to the fiscal year 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v 2.0, referred to as the "FY 2025 IG FISMA Reporting Metrics." We assessed the effectiveness of the Agency's information security program at Level 4 (Managed and Measurable). For those metrics that did not reach Level 4, we documented justifications. While we determined that the EPA has policies, procedures, and strategies implemented for these function areas and corresponding domains, improvements are needed in the following areas: • Tracking compliance with supply chain risk management control requirements – We found that the Agency has been unable to track compliance with the National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, Revision 5, supply chain risk management family of controls until updates to its governance, risk, and compliance tool are completed. • Maintaining a complete and accurate inventory of hardware assets connected to the Agency's network – We found that the Agency could not ensure a complete and accurate inventory of information technology hardware assets connected to its network through the U.S. Department of Homeland Security's Continuous Diagnostics and Mitigation program, in accordance with the National Institute of Standards and Technology Special Publication 800-53 control CM-8 ("System Component Inventory") and Cybersecurity and Infrastructure Security Agency Binding Operational Directive 23-01, Improving Asset Visibility and Vulnerability Detection on Federal Networks, due to issues with its asset discovery tool. • Tracking and resolving noncompliance with role-based training requirements for EPA personnel with significant IT responsibilities – We found that two employees in the system administrator role were not in compliance with role-based security training requirements for FY 2024 as provided by EPA information security procedures, and procedures were not followed to track the completion of their role-based security training requirements.

Function 1A: Govern - Cybersecurity Governance

1 **FY25 Supplemental.** To what extent does the organization develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize and communicate its cybersecurity objectives?
[CG.01]

Managed and Measurable (Level 4)

***Comments*:** Auditors conclude that the EPA has, in its program management procedures and practices, defined and implemented managed and measurable processes for developing and maintaining cybersecurity profiles that are used to understand, tailor, assess, prioritize, and communicate its cybersecurity objectives in fulfillment of FY 2025 IG FISMA Metric #1.

2 **FY25 Supplemental.** To what extent does the organization use a cybersecurity risk management strategy to support operational risk decisions?
[CG.02]

Managed and Measurable (Level 4)

***Comments*:** Auditors conclude that the EPA's cybersecurity risk management strategy supports operational risk decisions in fulfillment of FY 2025 IG FISMA Metric #2.

3 **FY25 Supplemental.** To what extent do cybersecurity roles, responsibilities, and authorities foster accountability, performance assessment, and continuous improvement?
[CG.03]

Managed and Measurable (Level 4)

***Comments*:** Auditors conclude that the EPA has, in its program management procedures and practices, defined and implemented managed and measurable processes to ensure that cybersecurity roles, responsibilities, and authorities are designed to foster accountability, performance assessment, and continuous improvement, in fulfillment of FY 2025 IG FISMA Metric #3.

4.1 Please provide the assessed maturity level for the agency's Govern - Cybersecurity Governance program.

Managed and Measurable (Level 4)

4.2 Provide any additional information on the effectiveness (positive or negative) of the organization's cybersecurity governance program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the cybersecurity governance program effective?
[CG.SUM]

We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics assessed at Level 4 that were not rated at Level 4, we documented justifications for those ratings.

Function 1B: Govern - Cybersecurity Supply Chain Risk Management (C-SCRM)

5 **FY25 Core.** To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?
[C-SCRM.01]

Consistently Implemented (Level 3)

***Comments*:** While the Agency is in the process of updating its governance, risk, and compliance tool from tracking NIST SP 800-53 Revision 4 to Revision 5 controls, OMB Circular No. A-130, Managing Information as a Strategic Resource, dated July 28, 2016, states that agencies must comply with NIST standards and guidelines. NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, Revision 5, September 2020 (with updates as of December 10, 2020), includes the supply chain risk management family of controls. For over 4 years, the EPA has been unable to track compliance with those controls pending the completion of GRC tool updates.

6.1 Please provide the assessed maturity level for the agency's Govern - Cybersecurity Supply Chain Risk Management (C-SCRM) program.
[GV.SUM]

Consistently Implemented (Level 3)

***Comments*:** We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics assessed at Level 4 that were not rated at Level 4, we documented justifications for those ratings.

6.2 Please provide the assessed maturity level for the agency's Govern program.

Managed and Measurable (Level 4)

***Comments*:** Since the "FY 2025 IG FISMA Reporting Metrics" gives inspectors general the discretion to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of the Govern function was Level 4 – (Managed and Measurable) based on the Calculated Average for FY 2025 metrics within the Govern function.

6.3 Provide any additional information on the effectiveness (positive or negative) of the organization's supply chain risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the supply chain risk management program effective?
[C-SCRM.SUM]

We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics assessed at Level 4 that were not rated at Level 4, we documented justifications for those ratings.

Function 2: Identify - Risk and Asset Management (RAM)

7 **FY25 Core.** To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections?
[RAM.01]

Defined (Level 2)

***Comments*:** This rating remains unchanged from the previous year's rating because corrective actions to address an FY 2024 finding on system inventory data validation related to this metric are not planned to be implemented until October 24, 2025.

8 **FY25 Core.** To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including Government Furnished Equipment (GFE), Internet of Things [IoT], and Bring Your Own Device [BYOD] mobile devices) connected to the organization`s network with the detailed information necessary for tracking and reporting?
[RAM.02]

Consistently Implemented (Level 3)

***Comments*:** The EPA has not fully implemented procedures to ensure a complete and accurate inventory of its IT hardware assets through the U.S. Department of Homeland Security's Continuous Diagnostics and Mitigation program in accordance with NIST SP 800-53 control CM-8 and CISA BOD 23-01 due to issues with the discovery tool not accurately identifying all network devices.

9 **FY25 Core.** To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?
[RAM.03]

Defined (Level 2)

***Comments*:** This rating remains unchanged from the previous year's rating because corrective actions to address an FY 2024 finding on software purchase data reconciliation related to this metric are not planned to be implemented until October 1, 2025.

10 **FY25 Supplemental.** To what extent does the organization develop and maintain inventories of data and corresponding metadata for designated data types, as appropriate throughout the data lifecycle?
[RAM.04]

Managed and Measurable (Level 4)

***Comments*:** Auditors conclude that the EPA has, in its risk management procedures and practices, implemented managed and measurable processes for developing and maintaining inventories of data and corresponding metadata for designated data types, as appropriate throughout the data lifecycle in fulfillment of FY 2025 IG FISMA Metric #10.

11 **FY25 Core.** To what extent does the organization ensure that information system security risks are adequately managed?
[RAM.05]

Managed and Measurable (Level 4)

***Comments*:** Auditors conclude that the EPA has, in its risk management practices and procedures, implemented managed and measured processes for using the results of its system level risk assessments, along with other inputs, to perform and maintain an organizationwide cybersecurity and privacy risk assessment in fulfillment of FY 2025 IG FISMA Metric #11.

12 **FY25 Core.** To what extent does the organization use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?
[RAM.06]

Managed and Measurable (Level 4)

***Comments*:** Auditors conclude that the EPA has, in its risk management practices and procedures, implemented a managed and measured process for a centralized, enterprisewide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards in fulfillment of FY 2025 IG FISMA Metric #12.

13.1 Please provide the assessed maturity level for the agency's Identify program.

Managed and Measurable (Level 4)

***Comments*:** Since the "FY 2025 IG FISMA Reporting Metrics" gives inspectors general the discretion to determine domain ratings by a calculated average scoring model, we determined that overall maturity of the Identify function was Level 4 – (Managed and Measurable) based on the Calculated Average for FY 2025 metrics within the Identify function.

13.2 Provide any additional information on the effectiveness (positive or negative) of the organization's RAM program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the RAM program effective?
[RAM.SUM]

We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics assessed at Level 4 that were not rated at Level 4, we documented justifications for those ratings.

Function 3A: Protect - Configuration Management

14 **FY25 Core.** To what extent does the organization use configuration settings/common secure configurations for its information systems?
[CM.01]

Consistently Implemented (Level 3)

***Comments*:** Based on the Agency response to corrective actions to address an FY 2024 finding related to baseline configuration failure tracking/remediation, the rollout for the automated reporting distribution will not occur until FY 2025's 4th quarter; therefore, we are unable to assess Level 4 (Managed and Measurable) for IG FISMA Metric #14 at this time.

15 **FY25 Core.** To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP-assets?
[CM.02]

Managed and Measurable (Level 4)

***Comments*:** Based on the previous year's rating of Level 4 (Managed and Measurable) and the lack of major changes to relevant IT processes and procedures, auditors conclude that the EPA has, in its information configuration management procedures and practices, implemented managed and measurable processes for using flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on network addressable IP-assets in fulfillment of FY 2025 IG FISMA Metric #15.

16.1 Please provide the assessed maturity level for the agency's Protect - Configuration Management program.

Managed and Measurable (Level 4)

16.2 Provide any additional information (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?
[CM.SUM]

We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics assessed at Level 4 that were not rated at Level 4, we documented justifications for those ratings.

Function 3B: Protect - Identity and Access Management (IDAM)

17 **FY25 Core.** To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for non-privileged users to access the organization`s physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access?
[IDAM-01]

Managed and Measurable (Level 4)

***Comments*:** Based on the previous year's rating of Level 4 (Managed and Measurable) and the lack of major changes to relevant IT processes and procedures, auditors conclude that the EPA has, in its identity and access management procedures and practices, implemented managed and measurable processes for phishing-resistant multifactor authentication mechanisms (for example, PIV, FIDO2, or web authentication) for non-privileged users to access the organization's physical and logical assets entry/exit points, networks, and systems, including for remote access, in fulfillment of FY 2025 IG FISMA Metric #17, through negative assurance.

18 **FY25 Core.** To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for privileged users to access the organization`s physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access?
[IDAM-02]

Managed and Measurable (Level 4)

***Comments*:** Based on the previous year's rating of Level 4 (Managed and Measurable) and the lack of major changes to relevant IT processes and procedures, auditors conclude that the EPA has, in its identity and access management procedures and practices, implemented managed and measurable processes for phishing-resistant multifactor authentication mechanisms (for example, PIV, FIDO2, or web authentication) for privileged users to access the organization's physical and logical assets entry/exit points, networks, and systems, including for remote access, in fulfillment of FY 2025 IG FISMA Metric #18, through negative assurance.

19 **FY25 Core.** To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed? [IDAM-03]

Managed and Measurable (Level 4)

***Comments*:** Auditors conclude that the EPA has, in its identity and access management practices and procedures, defined and implemented a managed and measurable process that ensures privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties, to include processes for periodic review and adjustment of privileged user accounts, and permissions, inventorying and validating the scope and number of privileged accounts and ensuring that privileged user account activities are logged and periodically reviewed in fulfillment of FY 2025 IG FISMA Metric #19.

20.1 Please provide the assessed maturity level for the agency's Protect - Identity and Access Management (IDAM) program.

Managed and Measurable (Level 4)

20.2 Provide any additional information (positive or negative) of the organization's IDAM program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the IDAM program effective?
[IDAM.SUM]

We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics assessed at Level 4 that were not rated at Level 4, we documented justifications for those ratings.

Function 3C: Protect - Data Protection and Privacy

21 **FY25 Core.** To what extent has the organization implemented the following security controls to protect the confidentiality, integrity, and availability of its PII and other agency sensitive data, as appropriate, throughout the data lifecycle?
• Encryption of data at rest
• Encryption of data in transit
• Limitation of transfer to removable media
• Sanitization of digital media prior to disposal or reuse
• Backups of data are created, protected, maintained, and tested
•Access to personal email, external file sharing and storage sites, and personal communication applications are blocked, as appropriate.
[DPP.01]

Managed and Measurable (Level 4)

***Comments*:** Based on the previous year's rating of Level 4 (Managed and Measurable) and the lack of major changes to relevant IT processes and procedures, auditors conclude that the EPA has, in its data protection and privacy procedures and practices, implemented managed and measurable processes for ensuring that the security controls for protecting personally identifiable information and other Agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's information security continuous monitoring strategy, in fulfillment of FY 2025 IG FISMA Metric #21, through negative assurance.

22 **FY25 Core.** To what extent has the organization implemented security controls (e.g., DLP, IDPS, CASB, User and Entity Behavior Analytic tools, SIEM and EDR) to prevent data exfiltration and enhance network defenses?
[DPP.02]

Managed and Measurable (Level 4)

***Comments*:** Based on the previous year's rating of Level 4 (Managed and Measurable) and the lack of major changes to relevant IT processes and procedures, auditors conclude that the EPA has, in its data protection and privacy procedures and practices, implemented managed and measurable processes for analyzing qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses, in fulfillment of FY 2025 IG FISMA Metric #22, through negative assurance.

23.1 Please provide the assessed maturity level for the agency's Protect - Data Protection and Privacy program.

Managed and Measurable (Level 4)

23.2 Provide any additional information (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?
[DPP.SUM]

Auditors conducted a review of the Agency's implementation of data protection and privacy procedures on the EPA's Enterprise Wide Area Network, in fulfillment of 42 U.S.C. § 2000ee-2: Privacy and data protection policies and procedures and noted the following: - Three out of the four (75%) tests conducted on the Agency's data loss prevention processes resulted in the failure of implemented controls to block fictitious Personally Identifiable Information sent to a nongovernment email address as part of the OIG's audit for data protection compliance with advance notice to the EPA. - Auditors' assessment of protection of data at rest via review of drive encryption, password encryption, and data exfiltration controls showed controls are in place to protect the resident data. Auditors recommend the EPA work with its vendor to review DLP controls and conduct periodic functional tests as needed to ensure its ability to prevent the leakage of sensitive data.

Function 3D: Protect - Security Training

24 **FY25 Core.** To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide specialized security training within the functional areas of: govern, identify, protect, detect, respond, and recover? [ST.01]?

Consistently Implemented (Level 3)

***Comments*:** Auditors found that two employees in the system administrator role were not in compliance with role-based security training requirements for FY 2024 as required by EPA information security procedure Directive No. CIO 2150-P-02.3, Information Security – Awareness and Training (AT) Procedure, dated June 12, 2023, and procedures were not followed to track the completion of their role-based security training requirements.

25.1 Please provide the assessed maturity level for the agency's Protect - Security Training program.

Consistently Implemented (Level 3)

***Comments*:** We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics assessed at Level 4 that were not rated at Level 4, we documented justifications for those ratings.

25.2 Please provide the assessed maturity level for the agency's Protect program.

Managed and Measurable (Level 4)

***Comments*:** Since the "FY 2025 IG FISMA Reporting Metrics" gives inspectors general the discretion to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of the Protect function was Level 4 – (Managed and Measurable) based on the Calculated Average for FY 2025 metrics within the Protect function.

25.3 Provide any additional information (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the security training program effective? [ST.SUM]

We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics assessed at Level 4 that were not rated at Level 4, we documented justifications for those ratings.

Function 4: Detect - Information Security Continuous Monitoring (ISCM)

26 **FY25 Core.** To what extent does the organization use information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?
[ISCM.01]

Managed and Measurable (Level 4)

***Comments*:** Based on the previous year's rating of Level 4 (Managed and Measurable) and the lack of major changes to relevant IT processes and procedures, auditors conclude that the EPA has, in its information security procedures and practices, implemented managed and measurable processes for ISCM strategy that addresses ISCM requirements and activities at each organizational tier defined, in fulfillment of FY 2025 IG FISMA Metric #26, through negative assurance.

27 **FY25 Supplemental.** To what extent does the organization monitor and measure the integrity and security posture of all owned and associated assets?
[ISCM.02]

Managed and Measurable (Level 4)

***Comments*:** Auditors conclude that the EPA has, in its information security procedures and practices, defined and consistently implemented processes for monitoring and measuring the integrity and security posture of owned and associated assets in fulfillment of FY 2025 IG FISMA Metric #27.

28 **FY25 Core.** To what extent does the organization performing ongoing (continuous monitoring) information system assessments to grant system authorizations, including developing and maintaining system security plans, and monitoring system security controls?
[ISCM.03]

Managed and Measurable (Level 4)

***Comments*:** Based on the previous year's rating of Level 4 (Managed and Measurable) and the lack of major changes to relevant IT processes and procedures, auditors conclude that the EPA has, in its information security procedures and practices, implemented managed and measurable processes for ongoing (continuous monitoring) information system assessments to grant system authorizations, including developing and maintaining system security plans, and monitoring system security controls, in fulfillment of FY 2025 IG FISMA Metric #28, through negative assurance.

29.1 Please provide the assessed maturity level for the agency's Detect program.

Managed and Measurable (Level 4)

***Comments*:** Since the "FY 2025 IG FISMA Reporting Metrics" gives inspectors general the discretion to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of the Detect function was Level 4 – (Managed and Measurable) based on the Calculated Average for FY 2025 metrics within the Detect function.

29.2 Provide any additional information (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the ISCM program effective? [ISCM.SUM]

We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics assessed at Level 4 that were not rated at Level 4, we documented justifications for those ratings.

Function 5: Respond - Incident Response

30 **FY25 Core.** To what extent has the organization implemented processes related to incident detection and analysis? [IR.01]

Managed and Measurable (Level 4)

***Comments*:** Auditors conclude that the EPA has, in its incident response procedures and practices, implemented managed and measurable processes related to incident detection and analysis in fulfillment of FY 2025 IG FISMA Metric #30.

31 **FY25 Core.** To what extent has the organization implemented processes related to incident handling? [IR.02]

Managed and Measurable (Level 4)

***Comments*:** Auditors conclude that the EPA has, in its incident response procedures and practices, implemented managed and measurable processes for incident handling in fulfillment of FY 2025 IG FISMA Metric #31.

32.1 Please provide the assessed maturity level for the agency's Respond program.

Managed and Measurable (Level 4)

***Comments*:** Since the "FY 2025 IG FISMA Reporting Metrics" gives inspectors general the discretion to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of the Respond function was Level 4 – (Managed and Measurable) based on the Calculated Average for FY 2025 metrics within the Respond function.

32.2 Provide any additional information (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the incident response program effective? [IR.SUM]

We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics assessed at Level 4 that were not rated at Level 4, we documented justifications for those ratings.

Function 6: Recover - Contingency Planning

33 **FY25 Core.** To what extent does the organization ensure that the results of BIAs are used to guide contingency planning efforts?
[CP.01]

Managed and Measurable (Level 4)

***Comments*:** Auditors conclude that the EPA has, in its contingency planning policies, procedures, and operations, implemented managed and measurable processes for using results of business impact analyses to guide contingency planning efforts in fulfillment of FY 2025 IG FISMA Metric #33.

34 **FY25 Core.** To what extent does the organization perform tests/exercises of its information system contingency planning processes?
[CP.02]

Managed and Measurable (Level 4)

***Comments*:** Auditors conclude that the EPA has, in its policies, contingency planning procedures, and operations, implemented managed and measurable processes for performing tests/exercises of its information system contingency planning processes in fulfillment of FY 2025 IG FISMA Metric #34.

35.1 Please provide the assessed maturity level for the agency's Recover program.

Managed and Measurable (Level 4)

***Comments*:** Since the "FY 2025 IG FISMA Reporting Metrics" gives inspectors general the discretion to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of the Recover function was Level 4 – (Managed and Measurable) based on the Calculated Average for FY 2025 metrics within the Recover function.

35.2 Provide any additional information (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the contingency planning program effective?
[CP.SUM]

We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics assessed at Level 4 that were not rated at Level 4, we documented justifications for those ratings.

APPENDIX A: Maturity Model Scoring

A.1 Please provide the assessed maturity level for the agency's Overall status.

Function	FY25 Core	FY25 Supplemental	FY25 Weighted Average	FY25 Assessed Maturity	FY25 Effectiveness	Explanation
Govern	3	4	3.86	Managed and Measurable (Level 4)	Effective	Since the "FY 2025 IG FISMA Reporting Metrics" gives inspectors general the discretion to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of the Govern function was Level 4 – (Managed and Measurable) based on the Calculated Average for FY 2025 metrics within the Govern function.

Function	FY25 Core	FY25 Supplemental	FY25 Weighted Average	FY25 Assessed Maturity	FY25 Effectiveness	Explanation
Identify	3	4	3	Managed and Measurable (Level 4)	Effective	Since the "FY 2025 IG FISMA Reporting Metrics" gives inspectors general the discretion to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of the Identify function was Level 4 – (Managed and Measurable) based on the Calculated Average for FY 2025 metrics within the Identify function.

Function	FY25 Core	FY25 Supplemental	FY25 Weighted Average	FY25 Assessed Maturity	FY25 Effectiveness	Explanation
Protect	3.75		3.75	Managed and Measurable (Level 4)	Effective	Since the "FY 2025 IG FISMA Reporting Metrics" gives inspectors general the discretion to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of the Protect function was Level 4 – (Managed and Measurable) based on the Calculated Average for FY 2025 metrics within the Protect function.
Detect	4	4	4	Managed and Measurable (Level 4)	Effective	
Respond	4		4	Managed and Measurable (Level 4)	Effective	
Recover	4		4	Managed and Measurable (Level 4)	Effective	

Function	FY25 Core	FY25 Supplemental	FY25 Weighted Average	FY25 Assessed Maturity	FY25 Effectiveness	Explanation
Overall Maturity	**3.63**	**4**	**3.77**	**Managed and Measurable (Level 4)**	**Effective**	

Appendix D

The EPA's FY 2025 FISMA Compliance Results

This table lists our assessment of the EPA's security function areas and domains, as well as the information security program's overall effectiveness.

Function area	Domain	OIG-assessed maturity level
Govern	Cybersecurity Governance	Level 4: managed and measurable
Govern	Cybersecurity Supply Chain Risk Management	Level 3: consistently implemented
Identify	Risk and Asset Management	Level 4: managed and measurable
Protect	Configuration Management	Level 4: managed and measurable
Protect	Identity and Access Management	Level 4: managed and measurable
Protect	Data Protection and Privacy	Level 4: managed and measurable
Protect	Security Training	Level 3: consistently implemented
Detect	Information Security Continuous Monitoring	Level 4: managed and measurable
Respond	Incident Response	Level 4: managed and measurable
Recover	Contingency Planning	Level 4: managed and measurable
Overall	—	**Level 4: managed and measurable**

Source: OIG assessment of the EPA's compliance with the OMB's *IG FISMA Reporting Metrics*. (EPA OIG table)

Agency Response to the Draft Report

OFFICE OF FINANCE AND ADMINISTRATION
WASHINGTON, D.C. 20460

April 30, 2026

MEMORANDUM

SUBJECT: Response to the Office of Inspector General Draft Report, Project No. OA-FY25-0041, *"Audit of the EPA's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2025"* dated April 3, 2026.

FROM: C. Paige Hanson, Chief Financial Officer and Chief Administrative Officer C. Paige Hanson

TO: Katherine Trimble, Assistant Inspector General
Office of Audit

Thank you for the opportunity to respond to the issues and recommendations in the subject draft audit report. Following is a summary of the U.S. Environmental Protection Agency's overall position, along with its position on each of the report's recommendations. We have provided high-level corrective actions and estimated completion dates.

AGENCY'S OVERALL POSITION

The agency concurs with the Office of Inspector General's findings, conclusions and recommendations. Under the annual assessment conducted by the OIG, EPA achieved an overall maturity rating of Level 4. This maturity rating indicates the program is "managed and measurable," meaning the EPA collects quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies across the organization and these measures are used to assess and make necessary changes.

The OIG put forth six recommendations in the following areas to improve overall operational effectiveness: Data Loss Prevention, Supply Chain Risk Management controls and Role-Based Training. EPA also recognizes the importance of continuous improvement and will implement the corrective action plans as described below and submit supporting documentation for recommendations that meet closeout criteria.

AGENCY'S RESPONSE TO DRAFT AUDIT RECOMMENDATIONS

Agreements

No.	Recommendation	High-Level Corrective Action(s)	Est. Completion Date
1	Implement controls to prevent and detect the transmission of all sensitive and confidential information by the data loss prevention tool. This effort would help correct data loss prevention gaps that allow the transmission of sensitive and confidential information outside the Agency's network.	Office of Finance and Administration-IT Operations Division will implement controls to prevent and detect the transmission of unencrypted sensitive and confidential information by the data loss prevention tool.	May 30, 2026
2	Develop and implement controls to periodically confirm the operating effectiveness of the data loss prevention tool's data transmission controls. This process would improve Agency oversight of the data loss prevention tool's data transmission controls.	OFA-ITOD will develop and implement controls to periodically confirm the operating effectiveness of the data loss prevention tool's data transmission controls.	July 17, 2026
3	Develop and implement a plan to complete updates of the EPA's system security plans to incorporate supply chain risk management security controls and requirements that align with National Institute of Standards and Technology Special Publication 800-53, Revision 5. These updates will establish supply chain risk management controls for each EPA system and allow the Agency to track and assess those controls	OFA-Cybersecurity, Privacy, and Risk Management Division will develop and implement a plan to complete updates of the EPA's system security plans to incorporate supply chain risk management security controls and requirements that align with National Institute of Standards and Technology Special Publication 800-53, Revision 5.	October 1, 2026

	to ensure operational effectiveness.		
4	Develop and implement controls to verify that service level agreements are established for EPA systems operated, in whole or part, by third-party vendors, as required by National Institute of Standards and Technology Special Publication 800-53, Revision 5. This will ensure that the vendors are adhering to National Institute of Standards and Technology controls to ensure the operational effectiveness of EPA systems.	OFA-CPRMD will develop and implement controls to verify that service-level agreements are established for EPA systems operated, in whole or in part, by third-party vendors, in accordance with NIST SP 800-53, Revision 5.	October 30, 2026
5	Annually instruct senior information officers or similar personnel in charge of employees to maintain a list identifying all their personnel with significant information technology security responsibilities, to certify the completeness and accuracy of this list, and to make these personnel aware of their role-based training requirements. This would improve Agency oversight by ensuring that only authorized personnel have access rights to EPA networks and systems.	OFA-CPRMD will annually instruct senior information officers or similar personnel in charge of employees to maintain a list identifying all their personnel with significant information technology security responsibilities, to certify the completeness and accuracy of this list, and to make these personnel aware of their role-based training requirements.	May 15, 2026
6	Develop and implement a process for senior information officers to periodically validate that their personnel with	OFA-CPRMD will develop and implement a process for senior information officers to periodically validate their personnel with significant	October 30, 2026

	significant information technology security responsibilities have completed the required role-based training. This process would improve the Agency's ability to prevent unauthorized access to the EPA network and safeguard its information and information systems.	information technology security responsibilities have completed the required role-based training.	

CONTACT INFORMATION

Thank you for the opportunity to review the report. If you have any questions regarding this response, please contact Afreeka Wilson, Audit Follow-up Coordinator, of the Office of Resources and Business Operations, (202) 564-0867 or wilson.afreeka@epa.gov.

Appendix F

Distribution List

The Administrator
Deputy Administrator
Associate Deputy Administrator
Assistant Deputy Administrator
Chief of Staff, Office of the Administrator
Deputy Chief of Staff for Management, Office of the Administrator
Agency Audit Follow-Up Official
Chief Financial Officer and Chief Administration Officer
Principal Deputy Chief Administrator Officer and Chief Acquisition Officer
Deputy Chief Financial Officer and Deputy Chief Administration Officer
Agency Audit Liaison
Agency Audit Follow-Up Coordinators
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for External Affairs
Deputy Associate Administrator for Public Affairs, Office of External Affairs
Director, Office of Resources and Information, Office of Finance and Administration
Controller, Office of Financial Operations & Management, Office of Finance and Administration
Deputy Controller, Office of Financial Operations & Management, Office of Finance and Administration
Director, Oversight & Accountability Division, Office of Financial Operations & Management, Office of Finance and Administration
OIG Liaison, Office of Policy and Regulatory Management, Office of the Administrator
GAO Liaison, Office of Policy and Regulatory Management, Office of the Administrator
Audit Follow-Up Coordinators

Whistleblower Protection

U.S. Environmental Protection Agency

The whistleblower protection coordinator's role is to educate Agency employees about prohibitions against retaliation for protected disclosures and the rights and remedies against retaliation. For more information, please visit our website.

Contact us:

Congressional & Media Inquiries: OIG.PublicAffairs@epa.gov

EPA OIG Hotline: OIG.Hotline@epa.gov

Web: epa.gov/oig

Follow us:

X: @epaoig

LinkedIn: linkedin.com/company/epa-oig

YouTube: youtube.com/epaoig

Instagram: @EPA_OIG

www.epa.gov/oig