

# Audit of the EPA's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2024

April 2, 2025 | Report No. 25-P-0023



## Report Contributors

Vincent Campbell  
LaVonda Harris  
Eric Jackson Jr.  
Sabrena Richardson  
Jeremy Sigel

## Abbreviations

CIO	Chief Information Officer
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
IG	Inspector General
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OISP	Office of Information Security and Privacy
OMB	Office of Management and Budget
SWAM	Software Asset Management

## Cover Image

The five security levels, with the EPA's overall maturity level (Level 4) highlighted, overlaying information security imagery. (EPA OIG images)

**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](mailto: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.epaoig.gov](http://www.epaoig.gov)

Subscribe to our [Email Updates](#).  
Follow us on X [@EPAoig](#).  
Send us your [Project Suggestions](#).



# At a Glance

## Audit of the EPA's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2024

### 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 fiscal year 2024 Inspector General Federal Information Security Modernization Act of 2014 reporting metrics.

The reporting metrics outline five security function areas and nine corresponding domains to help federal agencies manage cybersecurity risks. The document also outlines five maturity levels by which inspectors general should assess their agencies' information security programs. The EPA Office of Information Security and Privacy, which defines information security and privacy strategies, is a subset of the Office of Mission Support's Information Technology Security and Privacy Program that operated with a budget of about \$24 million in fiscal year 2024.

#### 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](mailto:OIG.PublicAffairs@epa.gov).

[List of OIG reports.](#)

### What We Found

We assessed the EPA's information security program effectiveness against the Office of Management and Budget's *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* at the maturity level of Level 4 (Managed and Measurable). The Agency achieved Level 4 ratings for 30, or 81 percent, of the 37 fiscal year 2024 metrics. Overall, we concluded that the EPA achieved a maturity level of Level 4 for the five security functions and nine domains outlined in the *IG FISMA Reporting Metrics*. This means that the EPA collects quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies across the organization that are used to assess and make necessary changes. We identified that the EPA had deficiencies in the following areas:

- Complete and accurate inventory of EPA information systems. We found that the Agency lacks a control to validate information system inventory data received from region and program offices prior to submission to the Office of Management and Budget.
- Software asset management data. We found that the Agency's software management asset tool lacks complete and accurate data related to its software license inventory.

**Without a complete and accurate inventory of information technology systems, software purchases, and licensing data, the Agency lacks accountability for and visibility of those assets on the Agency's network and limits opportunities to reduce duplicative license costs.**

### Recommendations and Planned Agency Corrective Actions

We recommend that the assistant administrator for Mission Support:

- Develop and implement procedures to reconcile its registry of applications with the governance, risk, and compliance tool.
- Develop and implement procedures for validating systems inventory data received by the region and program senior information officials.
- Designate a system of record for the EPA's software asset management and advise relevant personnel of that designation.

The Agency concurred with our recommendations and provided acceptable planned corrective actions with estimated milestone dates to address the recommendations. We consider these recommendations resolved with corrective actions pending.



**OFFICE OF INSPECTOR GENERAL**  
U.S. ENVIRONMENTAL PROTECTION AGENCY

April 2, 2025

**MEMORANDUM**

**SUBJECT:** Audit of the EPA's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2024  
Report No. 25-P-0023

**FROM:** Nicole N. Murley, Acting Inspector General *Nicole N. Murley*

**TO:** Michael Molina, Principal Deputy Assistant Administrator  
Office of Mission Support

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-FY24-0045. 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 Office of Mission Support is responsible for the issues discussed in this report.

In accordance with EPA Manual 2750, your office provided acceptable planned corrective actions and estimated milestone dates in response to OIG recommendations. All recommendations are resolved, and no final response to this report is required. If you submit a response, however, it will be posted on the OIG's website, along with our memorandum commenting on your response. Your 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 you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal along with corresponding justification.

We will post this report to our website at [www.epaoig.gov](http://www.epaoig.gov).

# Table of Contents

## Chapters

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
	Purpose.....	1
	Background.....	1
	Responsible Offices .....	3
	Scope and Methodology.....	4
	Prior Reports.....	4
<b>2</b>	<b>The EPA Needs to Validate Systems Inventory Data .....</b>	<b>6</b>
	The EPA Lacks a Documented Process for Validating Systems Inventory Data Prior to OMB Submission .....	6
	Recommendation .....	7
	Agency Response and OIG Assessment.....	7
<b>3</b>	<b>The EPA’s Software Asset Management Tool Contains Incomplete and Inaccurate Data for Its Software License Inventory.....</b>	<b>8</b>
	The EPA Needs to Update and Maintain Its Software License Inventory .....	8
	Recommendations.....	9
	Agency Response and OIG Assessment.....	9
<b>4</b>	<b>Status of Recommendations and Potential Monetary Benefits.....</b>	<b>10</b>

## Appendixes

<b>A</b>	<b>FY 2024 Core IG FISMA Reporting Metrics.....</b>	<b>11</b>
<b>B</b>	<b>FY 2024 Supplemental IG FISMA Reporting Metrics .....</b>	<b>13</b>
<b>C</b>	<b>OIG-Completed CyberScope Template .....</b>	<b>15</b>
<b>D</b>	<b>EPA FY 2024 FISMA Compliance Results .....</b>	<b>48</b>
<b>E</b>	<b>Agency Response to Draft Report .....</b>	<b>49</b>
<b>F</b>	<b>Distribution .....</b>	<b>52</b>

# 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 2024 inspector general, or IG, reporting metrics for the Federal Information Security Modernization Act of 2014, or FISMA.

### Background

According to the Office of Management and Budget, or OMB, FISMA requires agency heads to ensure that their respective agencies maintain information security protections that are:

[C]ommensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of (1) information collected or maintained by or on behalf of an agency or (2) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

FISMA also requires each IG to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of the respective agency. The OMB's *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.1, dated February 10, 2023, hereafter referred to as the *IG FISMA Reporting Metrics*, requires that 20 core metrics, which are listed in Appendix A, be assessed annually and the remaining supplemental metrics be assessed every two years. For FY 2024, there were 17 supplemental FISMA metrics, listed in Appendix B, to be assessed.

#### Function

According to the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1, a function is “[o]ne of the main components of the [Cybersecurity] Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five function areas are Identify, Protect, Detect, Respond, and Recover.”

#### Domain

National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, defines a domain as “[a]n environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.”

#### Metric






The *IG FISMA Reporting Metrics* identifies 66 metrics, which are questions divided among nine domains to provide reporting requirements across key areas to be addressed in the independent evaluations of agencies' information security programs.



As discussed in the *IG FISMA Reporting Metrics*, the core metrics represent a combination of presidential administration priorities, high-impact security processes, and essential functions necessary to determine information security program effectiveness. The supplemental metrics represent important activities conducted by information security programs and contribute to the overall evaluation and determination of the programs' effectiveness.

The *IG FISMA Reporting Metrics* align with the five function areas in the National Institute of Standards and Technology, or NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, dated April 16, 2018, hereafter referred to as the *Cybersecurity Framework*. As shown in Table 1, the five function areas are identify, protect, detect, respond, and recover. The *Cybersecurity Framework* provides a set of activities and guidance to achieve specific cybersecurity outcomes.

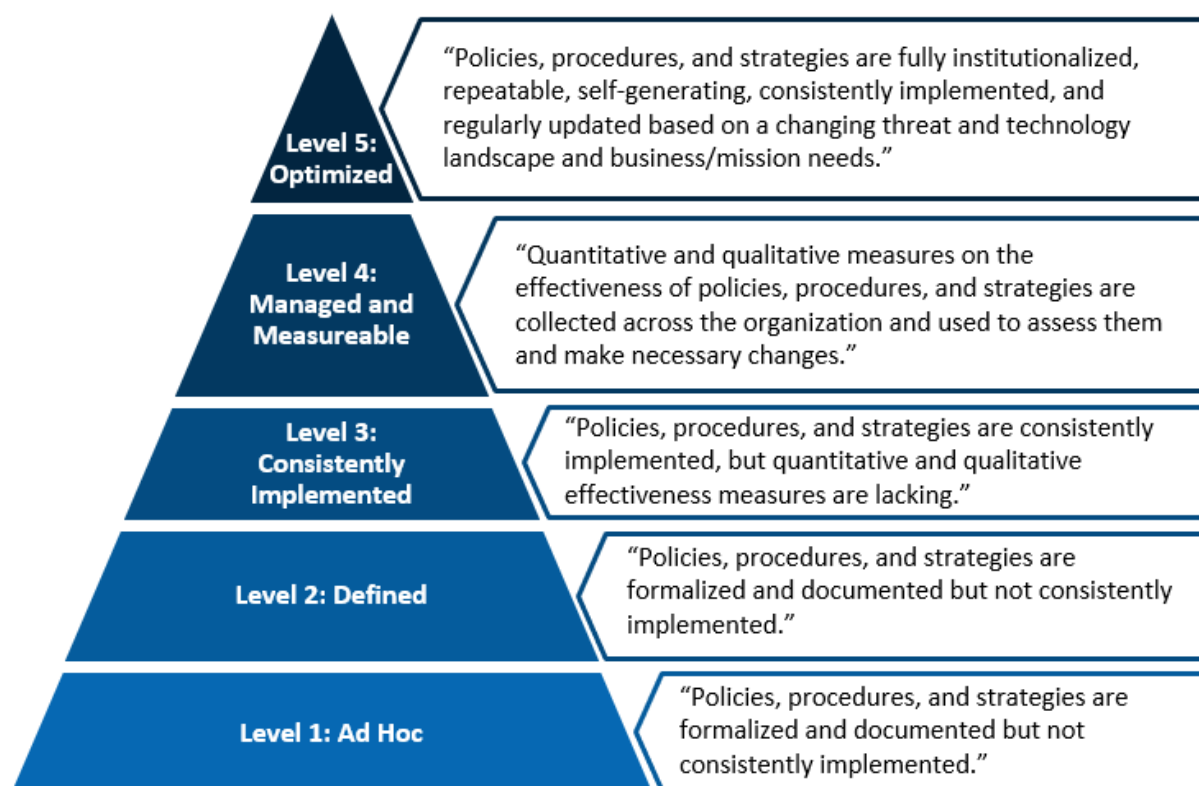
**Table 1: *IG FISMA Reporting Metrics* and *Cybersecurity Framework* function areas and categories**

	Domain	Related <i>Cybersecurity Framework</i> categories
	<b>Risk Management</b>	Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy
	<b>Supply Chain Risk Management</b>	Supply Chain Risk Management
	<b>Configuration Management</b>	Information Protection Processes and Procedures
	<b>Identity and Access Management</b>	Identity Management and Access Control
	<b>Data Protection and Privacy</b>	Data Security
	<b>Security Training</b>	Awareness and Training
	<b>Information Security Continuous Monitoring</b>	Security Continuous Monitoring
	<b>Incident Response</b>	Response Planning, Communications, Analysis, Mitigation, and Improvements
	<b>Contingency Planning</b>	Recovery Planning, Improvements, and Communications

Source: *IG FISMA Reporting Metrics* and *Cybersecurity Framework*. (EPA OIG table)

IGs are required to assess the effectiveness of information security programs on a maturity model spectrum in which the foundational levels ensure that agencies develop sound policies and procedures and in which the advanced levels capture the extent that agencies institutionalize those policies and procedures. The five maturity model levels are depicted in Figure 1.

**Figure 1: Maturity model spectrum**



Source: *IG FISMA Reporting Metrics*. (EPA OIG image)

Within the context of the maturity model, the OMB believes that achieving Level 4 (Managed and Measureable) or above represents an effective level of security. However, the *IG FISMA Reporting Metrics* provides that each OIG has the discretion to determine that its agency's information security program is effective even if the agency does not achieve Level 4.

## Responsible Offices

The Office of Mission Support leads the Agency's core mission support functions to improve efficiency, coordination, and customer experience for internal customers, stakeholders, and the public, including protecting the EPA's facilities and other critical assets nationwide, acquisition activities (contracts), grants management, human capital, information technology, and information management activities. It provides critical resources, tools, solutions, and support services that enable the EPA to protect human health and the environment.

The EPA's chief information security officer resides within the Office of Mission Support Office of Information Security and Privacy, or OISP. The OISP promotes agencywide cooperation in managing risks and protecting EPA information along with mission accomplishment. It defines clear, comprehensive, and enterprisewide information security and privacy strategies, including the program mission, vision, goals, objectives, and performance measures. Agency personnel stated that in FY 2024, the Office of



Mission Support was allocated a subset of \$23,889,000 of its overall budget to its Information Technology Security and Privacy Program, which includes the OISP.

## Scope and Methodology

We conducted this audit from February 2024 to January 2025 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 necessary to satisfy our audit objective.<sup>1</sup> In particular, we assessed internal control components—as outlined in the U.S. Government Accountability Office’s *Standards for Internal Control in the Federal Government*—significant to our audit objectives. Any internal control deficiencies we found are discussed in this report. Because our audit was limited to the internal control components deemed significant to our audit objective, it may not have disclosed all internal control deficiencies that may have existed at the time of the audit.

We assessed the EPA’s compliance with the 20 core and 17 supplemental IG FISMA metrics required for FY 2024. We assessed these 37 metrics at Maturity Level 4 (Managed and Measurable) for the domains within each FISMA security function area, which denotes that quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications for those ratings.

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 requested the EPA’s list of high-value assets, from which we selected the Office of Mission Support’s Enterprise Wide Area Network system. We assessed controls around the selected Enterprise Wide Area Network system for those metrics targeted at the system level.

We provided the Agency our assessment of each function area of the FY 2024 IG metrics and discussed the results. On July 29, 2024, we submitted the CyberScope Template to the OMB; this template can be found in Appendix C along with our assessment for each of the 37 IG metrics for FY 2024. Appendix D displays the individual domain ratings.

## Prior Reports

We 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*

---

<sup>1</sup> An entity designs, implements, and operates internal controls to achieve its objectives related to operations, reporting, and compliance. The U.S. Government Accountability Office sets internal control standards for federal entities in GAO-14-704G, *Standards for Internal Control in the Federal Government*, issued September 10, 2014.

*Inconsistently*, issued July 5, 2023. We recommended that the Agency update its policies to include a timely process for reviewing and updating information security procedures within a year of the issuance of relevant NIST publications. We also recommended that the Agency develop and implement a plan that included assigning responsibilities, as well as prioritizing and scheduling the installation of patches to address vulnerabilities in the Analytical Radiation Data System. We verified that the Agency developed (1) a policy to enforce a timely process for reviewing and updating information security procedures and (2) a plan to capture details for prioritizing and scheduling patches to be performed by the Analytical Radiation Data System owner. We consider these recommendations closed.

We also concluded that the corrective action associated with Recommendation 1 in EPA OIG Report No. [21-E-0124](#), *EPA Needs to Improve Processes for Updating Guidance, Monitoring Corrective Actions, and Managing Remote Access for External Users*, issued April 16, 2021, was completed at the time of our audit. We recommended that the Agency update information security procedures to make them consistent with current federal directives. We verified that the information security procedures have been updated. We consider this recommendation closed.

## Chapter 2

### The EPA Needs to Validate Systems Inventory Data

We found that the Agency lacks a control to validate systems inventory data to enforce Agency requirements. The Agency's information technology roles and responsibilities procedures require the chief information security officer to validate the content of FISMA submissions to the OMB, including system inventory numbers, but its *Systems Inventory Methodology* document, which guides the annual systems inventory process, does not include that step. Without validating the completeness and accuracy of its systems inventory, the Agency lacks assurance over the system inventory data submitted to the OMB.

#### The EPA Lacks a Documented Process for Validating Systems Inventory Data Prior to OMB Submission

We found that the Agency does not have a control to validate systems inventory data received from the region and program offices. The Agency's annual inventory methodology was established and implemented in FY 2023 with the *Systems Inventory Methodology*, version 1.0. This document was updated to Version 2.0 in February 2024 and outlines the process by which region and program offices review and update their system inventories, obtain approval from the senior information officer, and submit a signed memorandum to the OISP to include in the EPA inventory of information systems. However, the OISP could not provide evidence to support that the validation was actually performed.

Each agency should develop and update an inventory of organizational systems, according to NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, updated December 10, 2020, PM-5, "System Inventory." Additionally, this publication provides that each agency review and update the inventory on a frequency that the organization defines. In addition, the chief information security officer is responsible for validating CyberScope report content submitted to the OMB, including FISMA systems' inventory numbers, according to CIO-2150.3-P-19.2, *Information Security – Roles and Responsibilities Procedure*, dated May 19, 2022.

The lack of a control to validate the system inventory data occurred because the OISP's internal *Systems Inventory Methodology*, version 2.0, dated February 2024, does not include a procedure to require chief information security officer validation of system inventory data submitted to the OMB, as required in CIO-2150.3-P-19.2, *Information Security – Roles and Responsibilities Procedure*.

Without validation of Agency information technology systems inventory data, the Agency cannot ensure the completeness and accuracy of its systems inventory. Furthermore, without validating the inventory numbers, the Agency risks submitting incomplete or inaccurate data to the OMB.

## Recommendation

We recommend that the assistant administrator for Mission Support:

1. Develop and implement procedures for validating systems inventory data received by the region and program office senior information officers.

## Agency Response and OIG Assessment

The Agency's response to our draft report is in Appendix E. The EPA concurred with our recommendation and provided an acceptable planned corrective action and estimated milestone date.

The Agency concurred that it lacks documented procedures for validating the system inventory data received by region and program office senior information officers. We believe that the proposed corrective action will satisfy the intent of the recommendation. Therefore, we consider Recommendation 1 resolved with corrective action pending.

## Chapter 3

# The EPA's Software Asset Management Tool Contains Incomplete and Inaccurate Data for Its Software License Inventory

We found the Agency's software asset management, or SWAM, tool does not contain complete and accurate software license data needed to comply with NIST and Agency requirements. According to Agency personnel, this oversight occurred because the Agency's software procurement process does not require inputting purchase record information into the SWAM tool. Additionally, Agency personnel stated that the EPA has not designated a specific SWAM tool as the system of record for software license data. Without a complete and accurate inventory of software licenses, the Agency risks excessive spending on duplicative or unnecessary licenses.

### The EPA Needs to Update and Maintain Its Software License Inventory

EPA software license data in the Agency's SWAM tool are incomplete. As of August 22, 2024, we found that 128 purchased software license records were not matched to a software installation. As a result, the SWAM tool contained records for licenses that have either not been installed or have no matching installation record in the tool, relating to licenses worth about \$5.9 million. Additionally, 14 of the 128 purchases without matching installations did not have a license start or end date recorded to indicate the length of the license agreement.

Furthermore, the SWAM tool contained 1,543 software installations without matching purchases recorded. This set included 1,333, or 86 percent, of installations designated as "License Required" that did not state when the software license was purchased and when it will expire. NIST Special Publication 800-53, CM-10, "Software Usage Restrictions," provides that each agency should track the use of software and associated documentation protected by licenses. CIO 2150.3-P-05.2, *Information Security – Configuration Management (CM) Procedure*, dated June 12, 2023, implements this standard for all systems that require tracking software use and associated documentation protected by licenses. Agency personnel stated that the EPA's software procurement process does not require entering purchase record information into the Agency's SWAM tool. Furthermore, the Agency uses multiple tools to manage its software inventory and has not designated a single tool as the official system of record for software asset management.

Without a complete and accurate inventory of software purchase and licensing data, the Agency lacks accountability for, and visibility of, software installed on its network. This situation prevents the Agency from identifying opportunities to reduce costs on duplicative or unnecessary licenses and making informed investment decisions on its widely used software licenses.

## Recommendations

We recommend the assistant administrator for Mission Support:

2. Develop and implement procedures to reconcile software purchase data in the software asset management tool with software installations.
3. Document the software asset management tool's designation as the system of record for the Agency's enterprise software asset management and instruct senior information officials and relevant information technology personnel of that designation.

## Agency Response and OIG Assessment

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

The draft report recommended that the Agency develop and implement procedures to require responsible personnel to record software license information in the SWAM tool. Following discussions with the Agency, we determined that software management procedures require entering and maintaining software information in the Agency's software management system and that the SWAM tool automatically discovers software installed on the Agency network. However, the SWAM tool does not match purchased software with installations, and vice versa, leading to 1,543 software installations without matching purchases recorded in the tool. We updated Recommendation 2 to more directly address this issue; the Agency concurred with the revised recommendation and provided an acceptable planned corrective action and estimated milestone date. We consider this recommendation resolved with corrective action pending.

Additionally, the draft report recommended designating a system of record for the EPA's software asset management. The Agency responded that a communication was sent out on October 17, 2022, with that designation and proposed sending a reminder to senior information officers. We updated Recommendation 3 to document the system's designation in addition to sending a reminder to relevant information technology personnel. The Agency concurred with the revised recommendation and provided an acceptable planned corrective action and estimated milestone date. We consider this recommendation resolved with corrective action pending.



## Status of Recommendations and Potential Monetary Benefits

Rec. No.	Page No.	Recommendation	Status*	Action Official	Planned Completion Date	Potential Monetary Benefits (in \$000s)
1	7	Develop and implement procedures for validating systems inventory data received by the region and program office senior information officers.	R	Assistant Administrator for Mission Support	10/24/25	—
2	9	Develop and implement procedures to reconcile software purchase data in the software asset management tool with software installations.	R	Assistant Administrator for Mission Support	10/1/25	\$5,885
3	9	Document the software asset management tool's designation as the system of record for the Agency's enterprise software asset management and instruct senior information officials and relevant information technology personnel of that designation.	R	Assistant Administrator for Mission Support	4/15/25	—

\* C = Corrective action completed.

R = Recommendation resolved with corrective action pending.

U = Recommendation unresolved with resolution efforts in progress.

## FY 2024 Core IG FISMA Reporting Metrics

The numbers in the table correlate to the 66 metrics in the *IG FISMA Reporting Metrics*. The table only details the 20 core metrics that the IGs were required to assess for FY 2024.

Risk Management	
1.	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?
2.	To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?
3.	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?
5.	To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?
10.	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?
Supply Chain Risk Management	
14.	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?
Configuration Management	
20.	To what extent does the organization use configuration settings/common secure configurations for its information systems?
21.	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?
Identity and Access Management	
30.	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 facilities [organization-defined entry/exit points], networks, and systems, including for remote access?
31.	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 facilities [organization-defined entry/exit points], networks, and systems, including for remote access?
32.	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?

Data Protection and Privacy	
36.	To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? <ul style="list-style-type: none"> <li>• Encryption of data at rest</li> <li>• Encryption of data in transit</li> <li>• Limitation of transfer to removable media</li> <li>• Sanitization of digital media prior to disposal or reuse</li> </ul>
37.	To what extent has the organization implemented security controls (e.g., EDR) to prevent data exfiltration and enhance network defenses?
Security Training	
42.	To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?
Information Security Continuous Monitoring	
47.	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?
49.	How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls?
Incident Response	
54.	How mature are the organization's processes for incident detection and analysis?
55.	How mature are the organization's processes for incident handling?
Contingency Planning	
61.	To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?
63.	To what extent does the organization perform tests/exercises of its information system contingency planning processes?

Source: *IG FISMA Reporting Metrics*. (EPA OIG table)

## ***FY 2024 Supplemental IG FISMA Reporting Metrics***

The numbers in the table below correlate to the 66 metrics in the *IG FISMA Reporting Metrics*. The table only details the 17 supplemental metrics that IGs were required to assess for FY 2024.

<b>Risk Management</b>	
4.	To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets?
6.	To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain?
<b>Supply Chain Risk Management</b>	
15.	To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems?
<b>Configuration Management</b>	
17.	To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?
18.	To what extent does the organization use an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems?
23.	To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate?
<b>Identity and Access Management</b>	
28.	To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems?
<b>Data Protection and Privacy</b>	
38.	To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?
39.	To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements).
<b>Security Training</b>	
44.	To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting?)

45.	To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301)?
<b>Information Security Continuous Monitoring</b>	
50.	How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings?
<b>Incident Response</b>	
52.	To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents?
53.	To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?
56.	To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner?
<b>Contingency Planning</b>	
62.	To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?
64.	To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?

Source: *IG FISMA Reporting Metrics*. (EPA OIG table)

## *OIG-Completed CyberScope Template*

Inspector General

Section Report

2024

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 implements managed and measurable quantitative and qualitative measures on the effectiveness of policy, procedures, and strategies for all five information security function areas, which we have concluded effectively adhere to the "FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," hereafter referred to as the "FY 2023-2024 IG FISMA Reporting Metrics." We assessed the effectiveness of the Agency's information security program at Level 4. 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: (1) Complete and accurate inventory of EPA information systems. We found that the Agency's inventory of information systems in its registry of EPA applications, models, and data warehouses was not complete and accurate, as it did not include 13 systems listed in its governance, risk, and compliance tool. (2) Software asset management data. We found that the Agency's software asset management tool used to track software purchases lacks complete and accurate data related to its software license inventory.**

## Function 1A: Identify - Risk Management

- 1**      **FY24 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?

**Defined (Level 2)**

**Comments:** Auditors noted that the agency's inventory of information systems in its registry of EPA applications, models, and data warehouses was not complete and accurate, as it did not include 13 systems listed in its governance, risk, and compliance tool.
- 2**      **FY24 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 GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?

**Defined (Level 2)**

**Comments:** This rating remains unchanged from the previous year's rating because corrective actions to address FY 2023 findings related to this metric are not planned to be implemented until January 15, 2025.
- 3**      **FY24 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?

**Defined (Level 2)**

**Comments:** Auditors noted the Agency's software asset management tool used to track software purchases lacks complete and accurate data related to its software license inventory.
- 4**      **FY24 Supplemental.** To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 11.2.

- 5 **FY24 Core.** To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 11.2.

- 6 **FY24 Supplemental.** To what extent does the organization use an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 11.2.

- 7 **FY23 Supplemental.** To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, implemented, and appropriately resourced across the organization?

**Managed and Measurable (Level 4)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 8 **FY23 Supplemental.** To what extent has the organization ensured that plans of action and milestones (POA&Ms) are used for effectively mitigating security weaknesses?

**Managed and Measurable (Level 4)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 9 **FY23 Supplemental.** To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders?

**Managed and Measurable (Level 4)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 10 **FY24 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?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 11.2.

- 11.1 Please provide the assessed maturity level for the agency's Identify - Risk Management program.

**Consistently Implemented (Level 3)**

**Comments:** Since the "FY 2023-2024 IG FISMA Reporting Metrics" requires inspectors general to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of Risk Management was Level 3 based on Calculated Average for Risk Management Metrics Maturity calculations.

- 11.2 Provide any additional information on the effectiveness (positive or negative) of the organizations 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 risk management program effective?

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

## Function 1B: Identify - Supply Chain Risk Management

- 12 FY23 Supplemental.** To what extent does the organization use an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?

**Defined (Level 2)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 13 FY23 Supplemental.** To what extent does the organization use SCRM policies and procedures to manage SCRM activities at all organizational tiers?

**Ad Hoc (Level 1)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 14 FY24 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?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 16.3.

- 15 FY24 Supplemental.** To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 16.3.

**16.1** Please provide the assessed maturity level for the agency's Identify - Supply Chain Risk Management program.

**Managed and Measurable (Level 4)**

**Comments:** Since the "FY 2023-2024 IG FISMA Reporting Metrics" requires inspectors general to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of Supply Chain Risk Management was Level 4 based on Calculated Average for Supply Chain Risk Management Metrics Maturity calculations.

**16.2** Please provide the assessed maturity level for the agency's Identify Function.

**Managed and Measurable (Level 4)**

**Comments:** Since the "FY 2023-2024 IG FISMA Reporting Metrics" requires inspectors general to determine function effectiveness by a calculated average scoring model, we determined that the overall maturity of the Identify Function was Level 4 based on Calculated Average for Identify Function Metrics Maturity calculations.

**16.3** Provide any additional information on the effectiveness (positive or negative) of the organizations 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?

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



## Function 2A: Protect - Configuration Management

- 17 **FY24 Supplemental.** To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?
- Managed and Measurable (Level 4)**
- Comments:** See remarks in question 25.2.
- 18 **FY24 Supplemental.** To what extent does the organization use an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems?
- Managed and Measurable (Level 4)**
- Comments:** See remarks in question 25.2.
- 19 **FY23 Supplemental.** To what extent does the organization use baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting?
- Defined (Level 2)**
- Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.
- 20 **FY24 Core.** To what extent does the organization use configuration settings/common secure configurations for its information systems?
- Defined (Level 2)**
- Comments:** This rating remains unchanged from the previous year's rating because corrective actions to address FY 2023 findings related to this metric are not planned to be implemented until November 1, 2024.

- 21**      **FY24 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?
- Managed and Measurable (Level 4)**
- Comments:** See remarks in question 25.2.
- 22**      **FY23 Supplemental.** To what extent has the organization adopted the Trusted Internet Connection (TIC) 3.0 program to assist in protecting its network?
- Defined (Level 2)**
- Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.
- 23**      **FY24 Supplemental.** To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate?
- Managed and Measurable (Level 4)**
- Comments:** See remarks in question 25.2.
- 24**      **FY23 Supplemental.** To what extent does the organization use a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet- accessible federal systems?
- Consistently Implemented (Level 3)**
- Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

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

**Managed and Measurable (Level 4)**

**Comments:** Since the "FY 2023-2024 IG FISMA Reporting Metrics" requires inspectors general to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of Configuration Management was Level 4 based on Calculated Average for Configuration Management Metrics Maturity calculations.

**25.2** Provide any additional information on the effectiveness (positive or negative) of the organizations configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?

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

## Function 2B: Protect - Identity and Access Management

- 26 FY23 Supplemental.** To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?

**Managed and Measurable (Level 4)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 27 FY23 Supplemental.** To what extent does the organization use a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities?

**Consistently Implemented (Level 3)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 28 FY24 Supplemental.** To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 34.2.

- 29 FY23 Supplemental.** To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained?

**Managed and Measurable (Level 4)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 30**      **FY24 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 facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 34.2.

- 31**      **FY24 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 facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 34.2.

- 32**      **FY24 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?

**Consistently Implemented (Level 3)**

**Comments:** Auditors assessed this metric at Level 3, as the Agency is currently working on corrective actions related to implementing Event Logging 2, or EL2, as outlined in Office of Management and Budget Memorandum M-21-31. The Agency plans to complete this corrective action by August 15, 2024.

- 33**      **FY23 Supplemental.** To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions?

**Managed and Measurable (Level 4)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

**34.1** Please provide the assessed maturity level for the agency's Protect - Identity and Access Management program.

**Managed and Measurable (Level 4)**

**Comments:** Since the "FY 2023-2024 IG FISMA Reporting Metrics" requires inspectors general to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of Identity and Access Management was Level 4 based on Calculated Average for Identity and Access Management Metrics Maturity calculations.

**34.2** Provide any additional information on the effectiveness (positive or negative) of the organizations identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?

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

## Function 2C: Protect - Data Protection and Privacy

- 35 FY23 Supplemental.** To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems?

**Managed and Measurable (Level 4)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 36 FY24 Core.** To what extent has the organization implemented the following security controls to protect 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

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 40.2.

- 37 FY24 Core.** To what extent has the organization implemented security controls (e.g., EDR) to prevent data exfiltration and enhance network defenses?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 40.2.

- 38 FY24 Supplemental.** To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 40.2.



- 39** **FY24 Supplemental.** To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training?(Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and user requirements)

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 40.2.

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

**Managed and Measurable (Level 4)**

**Comments:** Since the "FY 2023-2024 IG FISMA Reporting Metrics" requires inspectors general to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of Data Protection and Privacy was Level 4 based on Calculated Average for Data Protection and Privacy Metrics Maturity calculations.

- 40.2** Provide any additional information on the effectiveness (positive or negative) of the organizations data protection and privacy program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?

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

## Function 2D: Protect - Security Training

- 41 FY23 Supplemental.** To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced? Note: This includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities.

### Managed and Measurable (Level 4)

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 42 FY24 Core.** To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?

### Managed and Measurable (Level 4)

**Comments:** See remarks in question 46.3.

**43 FY23 Supplemental.** To what extent does the organization use a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment? Note: The strategy/plan should include the following components:

- The structure of the awareness and training program
- Priorities
- Funding
- The goals of the program
- Target audiences
- Types of courses/ material for each audience
- Use of technologies (such as email advisories, intranet updates/wiki pages/social media, web- based training, phishing simulation tools)
- Frequency of training
- Deployment methods

**Ad Hoc (Level 1)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

**44 FY24 Supplemental.** To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting?)

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 46.3.

- 45 FY24 Supplemental.** To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization's security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301)?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 46.3.

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

**Managed and Measurable (Level 4)**

**Comments:** Since the "FY 2023-2024 IG FISMA Reporting Metrics" requires inspectors general to determine domain ratings by a calculated average scoring model, we determined that the overall maturity of Security Training was Level 4 based on Calculated Average for Security Training Metrics Maturity calculations.

- 46.2** Please provide the assessed maturity level for the agency's Protect Function.

**Managed and Measurable (Level 4)**

**Comments:** Since the "FY 2023-2024 IG FISMA Reporting Metrics" requires inspectors general to determine function effectiveness by a calculated average scoring model, we determined that the overall maturity of the Protect Function was Level 4 based on Calculated Average for Protect Function Metrics Maturity calculations.

- 46.3** Provide any additional information on the effectiveness (positive or negative) of the organizations security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?

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

### Function 3: Detect - ISCM

- 47 FY24 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?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 51.2.

- 48 FY23 Supplemental.** To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?

**Managed and Measurable (Level 4)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 49 FY24 Core.** How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 51.2.

- 50 FY24 Supplemental.** How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 51.2.

**51.1** Please provide the assessed maturity level for the agency's Detect - ISCM function.

**Managed and Measurable (Level 4)**

**Comments:** Since the "FY 2023-2024 IG FISMA Reporting Metrics" requires inspectors general to determine function ratings by a calculated average scoring model, we determined that the overall maturity of the Detect - ISCM Function was Level 4 based on Calculated Average for ISCM Metrics Maturity calculations.

**51.2** Provide any additional information on the effectiveness (positive or negative) of the organizations ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?

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

## Function 4: Respond - Incident Response

- 52 FY24 Supplemental.** To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 59.2.

- 53 FY24 Supplemental.** To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 59.2.

- 54 FY24 Core.** How mature are the organization's processes for incident detection and analysis?

**Defined (Level 2)**

**Comments:** This rating remains unchanged from the previous year's rating because corrective actions to address FY 2023 findings related to this metric are not planned to be implemented until August 15, 2024.

- 55 FY24 Core.** How mature are the organization's processes for incident handling?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 59.2.

- 56 FY24 Supplemental.** To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 59.2.

- 57 FY23 Supplemental.** To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support?

**Managed and Measurable (Level 4)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 58 FY23 Supplemental.** To what extent does the organization use the following technology to support its incident response program?

- Web application protections, such as web application firewalls
- Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools
- Aggregation and analysis, such as security information and event management (SIEM) products
- Malware detection, such as antivirus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools

**Consistently Implemented (Level 3)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.



**59.1** Please provide the assessed maturity level for the agency's Respond - Incident Response function.

**Managed and Measurable (Level 4)**

**Comments:** Since the "FY 2023-2024 IG FISMA Reporting Metrics" requires inspectors general to determine function ratings by a calculated average scoring model, we determined that the overall maturity of Respond - Incident Response Function was Level 4 based on Calculated Average for Incident Response Metrics Maturity calculations.

**59.2** Provide any additional information on the effectiveness (positive or negative) of the organizations incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?

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

## Function 5: Recover - Contingency Planning

- 60 FY23 Supplemental.** To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority?

**Managed and Measurable (Level 4)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 61 FY24 Core.** To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 66.2.

- 62 FY24 Supplemental.** To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 66.2.

- 63 FY24 Core.** To what extent does the organization perform tests/exercises of its information system contingency planning processes?

**Managed and Measurable (Level 4)**

**Comments:** See remarks in question 66.2.

- 64** **FY24 Supplemental.** To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?

**Consistently Implemented (Level 3)**

**Comments:** Auditors noted two out of four sampled systems had control-type discrepancies related to Contingency Planning controls identified by the Security Control Assessor in the Security Assessment Reports that were not remediated or tracked via plans of actions and milestones as required by section CA-5 of the Agency's Information Security - Assessment, Authorization, and Monitoring (CA) Procedure, CIO 2150-P-04.3.

- 65** **FY23 Supplemental.** To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk-based decisions?

**Consistently Implemented (Level 3)**

**Comments:** The "FY 2023-2024 IG FISMA Reporting Metrics" requires that these metrics be evaluated on a two-year cycle; therefore, we did not include their ratings in the calculation of FY 2024 effectiveness.

- 66.1** Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.

**Managed and Measurable (Level 4)**

**Comments:** Since the "FY 2023-2024 IG FISMA Reporting Metrics" requires inspectors general to determine function ratings by a calculated average scoring model, we determined that the overall maturity of Recover - Contingency Planning Function was Level 4 based on Calculated Average for Contingency Planning Metrics Maturity calculations.

- 66.2** Provide any additional information on the effectiveness (positive or negative) of the organizations contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?

**We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics that were assessed at Level 4 but 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	Core	FY23 Supplemental	FY24 Supplemental	FY24 Assessed Maturity	FY24 Effectiveness	Explanation
Identify	3.00	3.00	4.00	Managed and Measurable (Level 4)	Effective	We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics that were assessed at Level 4 but were not rated at Level 4, we documented justifications for those ratings.
Protect	3.63	3.10	4.00	Managed and Measurable (Level 4)	Effective	We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics that were assessed at Level 4 but were not rated at Level 4, we documented justifications for those ratings.
Detect	4.00	4.00	4.00	Managed and Measurable (Level 4)	Effective	We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics that were assessed at Level 4 but were not rated at Level 4, we documented justifications for those ratings.

Function	Core	FY23 Supplemental	FY24 Supplemental	FY24 Assessed Maturity	FY24 Effectiveness	Explanation
Respond	3.00	3.50	4.00	Managed and Measurable (Level 4)	Effective	We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics that were assessed at Level 4 but were not rated at Level 4, we documented justifications for those ratings.
Recover	4.00	3.50	3.50	Managed and Measurable (Level 4)	Effective	We assessed the effectiveness of the Agency's information security program at Level 4. For those metrics that were assessed at Level 4 but were not rated at Level 4, we documented justifications for those ratings.

Function	Core	FY23 Supplemental	FY24 Supplemental	FY24 Assessed Maturity	FY24 Effectiveness	Explanation
Overall Maturity	3.53	3.42	3.90	Managed and Measurable (Level 4)	Effective	<p>The U.S. Environmental Protection Agency Office of Inspector General determined that, overall, the EPA has demonstrated that it implements managed and measurable quantitative and qualitative measures on the effectiveness of policy, procedures, and strategies for all five information security function areas, which we have concluded effectively adhere to the “FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics,” hereafter referred to as the “FY 2023-2024 IG FISMA Reporting Metrics.” We assessed the effectiveness of the Agency’s information security program at Level 4. 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</p>

Function	Core	FY23 Supplemental	FY24 Supplemental	FY24 Assessed Maturity	FY24 Effectiveness	Explanation
						<p>following areas:</p> <p>(1) Complete and accurate inventory of EPA information systems. We found that the Agency's inventory of information systems in its registry of EPA applications, models, and data warehouses was not complete and accurate, as it did not include 13 systems listed in its governance, risk, and compliance tool.</p> <p>(2) Software asset management data. We found that the Agency's software asset management tool used to track software purchases lacks complete and accurate data related to its software license inventory.</p>

#### Function 1A: Identify - Risk Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	3	0
Consistently Implemented (Level 3)	0	0

Managed and Measurable (Level 4)	2	2
Optimized (Level 5)	0	0
<b>Calculated Rating:</b>	<b>2.80</b>	<b>4.00</b>

#### Function 1B: Identify - Supply Chain Risk Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	1	1
Optimized (Level 5)	0	0
<b>Calculated Rating:</b>	<b>4.00</b>	<b>4.00</b>

#### Function 2A: Protect - Configuration Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	0
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	1	3



Optimized (Level 5)	0	0
<b>Calculated Rating:</b>	<b>3.00</b>	<b>4.00</b>

#### Function 2B: Protect - Identity and Access Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	1	0
Managed and Measurable (Level 4)	2	1
Optimized (Level 5)	0	0
<b>Calculated Rating:</b>	<b>3.67</b>	<b>4.00</b>

#### Function 2C: Protect - Data Protection and Privacy

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	2	2
Optimized (Level 5)	0	0

<b>Calculated Rating:</b>	<b>4.00</b>	<b>4.00</b>
---------------------------	-------------	-------------

#### Function 2D: Protect - Security Training

<b>Maturity Level</b>	<b>Core</b>	<b>Supplemental</b>
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	1	2
Optimized (Level 5)	0	0
<b>Calculated Rating:</b>	<b>4.00</b>	<b>4.00</b>

#### Function 3: Detect - ISCM

<b>Maturity Level</b>	<b>Core</b>	<b>Supplemental</b>
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	2	1
Optimized (Level 5)	0	0
<b>Calculated Rating:</b>	<b>4.00</b>	<b>4.00</b>

**Function 4: Respond - Incident Response**

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	0
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	1	3
Optimized (Level 5)	0	0
<b>Calculated Rating:</b>	<b>3.00</b>	<b>4.00</b>

**Function 5: Recover - Contingency Planning**

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	0	0
Consistently Implemented (Level 3)	0	1
Managed and Measurable (Level 4)	2	1
Optimized (Level 5)	0	0
<b>Calculated Rating:</b>	<b>4.00</b>	<b>3.50</b>

## ***EPA FY 2024 FISMA Compliance Results***

### **Overall maturity level and assessment of the EPA's security function areas and domains**

<b>Security function</b>	<b>Security domain</b>	<b>OIG-assessed maturity level</b>
Identify	Risk Management	Level 3: Consistently Implemented
Identify	Supply Chain Risk 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 4: Managed and Measurable
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
—	<b>The EPA's overall maturity rating:</b>	<b>Level 4: Managed and Measurable</b>

Source: OIG overall maturity rating and assessment results by information security function and domain.  
(EPA OIG table)

## *Agency Response to Draft Report*



### OFFICE OF MISSION SUPPORT

WASHINGTON, D.C. 20460

March 7, 2025

#### MEMORANDUM

**SUBJECT:** Response to the Office of Inspector General Draft Report, Project No. OA-FY24-0045, *"The EPA Achieved an Effective Rating for the Federal Information Security Modernization Act for Fiscal Year 2024 but Needs to Improve Its Systems Inventory and Software License Data Tracking Processes"* dated January 27, 2025.

**FROM:** Vaughn Noga, Chief Information Officer  
Deputy Assistant Administrator for Information Technology and Information Management  
Office of Mission Support

**TO:** Michelle Wicker, Director  
Information Resources Management  
Office of Audit

VAUGHN NOGA

Digitally signed by VAUGHN  
NOGA  
Date: 2025.03.07 06:40:11 -05'00'

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 recommendation 1, as well as the updated recommendations 2 and 3.

## AGENCY'S RESPONSE TO DRAFT AUDIT RECOMMENDATIONS

### Agreements

No.	Recommendation	High-Level Corrective Action(s)	Est. Completion Date
1	Develop and implement procedures for validating systems inventory data received by the region and program office senior information officers.	OMS-OISP will develop and validate system inventory data received by the region and program office senior information officers.	October 24, 2025
2	Develop and implement procedures to reconcile software purchase data in the software asset management system with software installations.	OMS-OITO will launch an awareness program in April through September to ensure all software license information is recorded in the Agency's centralized software asset management system or provide training on the procedures.	October 1, 2025
3	Document the software asset management tool's designation as the system of record for the Agency's enterprise software asset management and instruct Senior Information Officials and other relevant IT personnel of that designation	OMS-OITO will send communication to programs and regions reminding them of the requirement to record software licenses in the Agency's centralized software asset management system. The communication will include planned training opportunities for key personnel.	April 15, 2025

### 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](mailto:wilson.afreeka@epa.gov).

cc:

Vincent Campbell  
LaVonda Harris  
Eric Jackson, Jr.  
Sabrena Richardson  
Jeremy Sigel  
Erin Collard  
David Alvarado

Austin Henderson  
Tonya Manning  
Mark Bacharach  
Lee Kelly  
Kaitlyn Khan  
Tiffany McNeill  
Bob Vojtik  
DeShelia Hall  
Mojgan Rahai  
Yulia Kalikhman  
Gregory Scott  
Jan Jablonski  
Justin Bossard  
Afreeka Wilson  
Darryl Perez  
Susan Perkins  
Andrew LeBlanc  
Jose Kercado-Deleon

## *Distribution*

The Administrator  
Deputy Administrator  
Assistant Deputy Administrator  
Associate Deputy Administrator  
Chief of Staff, Office of the Administrator  
Deputy Chief of Staff for Management, Office of the Administrator  
Assistant Administrator for Mission Support  
Agency Follow-Up Official (the CFO)  
Agency Follow-Up Coordinator  
General Counsel  
Associate Administrator for Congressional and Intergovernmental Relations  
Associate Administrator for Public Affairs  
Principal Deputy Associate Administrator for Public Affairs  
Principal Deputy Assistant Administrator for Mission Support  
Chief Information Officer and Deputy Assistant Administrator for Information Technology and  
Information Management, Office of Mission Support  
Deputy Assistant Administrator for Mission Support Programs  
Deputy Assistant Administrator for Workforce Solutions, Office of Mission Support  
Deputy Assistant Administrator for Infrastructure and Extramural Resources, Office of Mission Support  
Director, Office of Resources and Business Operations, Office of Mission Support  
Director, Office of Continuous Improvement, Office of the Chief Financial Officer  
Director and Chief Information Security Officer, Office of Information Security and Privacy, Office of  
Mission Support  
OIG Liaison, Office of Policy, Office of the Administrator  
GAO Liaison, Office of Policy, Office of the Administrator  
Audit Follow-Up Coordinator, Office of the Administrator  
Audit Follow-Up Coordinator, Office of Mission Support





## 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 the OIG's whistleblower protection [webpage](#).*

### Contact us:



**Congressional & Media Inquiries:** [OIG.PublicAffairs@epa.gov](mailto:OIG.PublicAffairs@epa.gov)



**EPA OIG Hotline:** [OIG.Hotline@epa.gov](mailto:OIG.Hotline@epa.gov)



**Web:** [epaoig.gov](http://epaoig.gov)

### Follow us:



**X:** [@epaoig](https://twitter.com/epaoig)



**LinkedIn:** [linkedin.com/company/epa-oig](https://www.linkedin.com/company/epa-oig)



**YouTube:** [youtube.com/epaoig](https://www.youtube.com/epaoig)



**Instagram:** [@epa.ig.on.ig](https://www.instagram.com/epa.ig.on.ig)



[www.epaoig.gov](http://www.epaoig.gov)