# The EPA Needs to Develop and Implement Information Technology Processes to Comply with the Federal Information Security Modernization Act for Fiscal Year 2023

August 5, 2024 | Report No. 24-P-0052


OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

## Report Contributors

LaSharn Barnes
LaVonda Harris
Eric Jackson Jr.
Sabrena Richardson
Jeremy Sigel

## Abbreviations

| | |
|---|---|
| CIO | Chief Information Officer |
| EL1 | Event Logging Tier 1 |
| EL2 | Event Logging Tier 2 |
| EPA | U.S. Environmental Protection Agency |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Modernization Act |
| FY | Fiscal Year |
| IG | Inspector General |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| RMF | Risk Management Framework |
| SP | Special Publication |

## Key Definitions

*Please see Appendix A for key definitions.*

## Cover Image

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

24-P-0052
August 5, 2024

# At a Glance

# *The EPA Needs to Develop and Implement Information Technology Processes to Comply with the Federal Information Security Modernization Act for Fiscal Year 2023*

## 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 2023 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 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 $25 million in fiscal year 2023.

**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 concluded that the EPA achieved an overall maturity level of Level 3, Consistently Implemented, for the five security functions and nine domains outlined in the Office of Management and Budget's *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*. This means that the EPA consistently implemented its information security policies and procedures, but quantitative and qualitative effectiveness measures are lacking. We identified that the EPA had deficiencies in the following areas:

- Establishing the information security documentation related to supply chain risk management procedures, finalizing a security training and awareness plan, updating the *Information Security Continuous Monitoring Strategic Plan*, and ensuring that all documents and procedures comply with the latest federal guidance issued by the National Institute of Standards and Technology.
- Implementing information technology, or IT, processes to comply with event logging requirements for the detection of incidents and discovery of unauthorized hardware on the Agency's network.
- Developing internal controls to verify the completeness and accuracy of the Agency's IT asset inventory, remediating information systems' configuration compliance findings, and ensuring the accuracy of the information systems' security objective risk levels in the Agency's Risk Management Framework tool.

**Without fully documented, implemented, and compliant IT procedures, the Agency cannot ensure that its information security program is protecting EPA systems and data to adhere to the National Institute of Standards and Technology standards.**

## Recommendations and Planned Agency Corrective Actions

We made nine recommendations to the assistant administrator for Mission Support. The Agency concurred with our recommendations, completed corrective actions for five recommendations, and provided acceptable planned corrective actions with estimated milestone dates for the remaining four recommendations. We also made revisions to Recommendation 8 in response to Agency comments to the draft report which the Agency agreed with and provided acceptable planned corrective actions with estimated milestone dates. We consider the remaining four recommendations resolved with corrective actions pending.

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

August 5, 2024

**MEMORANDUM**

**SUBJECT:** The EPA Needs to Develop and Implement Information Technology Processes to Comply with the Federal Information Security Modernization Act for Fiscal Year 2023
Report No. 24-P-0052

**FROM:** Sean W. O'Donnell, Inspector General

**TO:** Kimberly Patrick, 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 project was OA-FY23-0061. 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 completed corrective actions for Recommendations 1, 2, 6, 7, and 9. Your office also provided acceptable planned corrective actions and milestone dates in response to Recommendations 3, 4, 5, and 8. These four recommendations are resolved with corrective actions pending. A final response pertaining to the nine recommendations is not required; however, if you submit a response, 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 accessibility 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.

# *Table of Contents*

## Chapters



*–continued–*

# 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 2023 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.

**Security Program**

National Institute of Standards and Technology Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model,* dated April 1998, defines a security program as "a program established, implemented, and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated" in its information technology systems.

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 the 20 core metrics, which are in Appendix B, be assessed annually and the remaining supplemental metrics be assessed every two years. For FY 2023, there were 20 supplemental FISMA metrics, listed in Appendix C, to be assessed.

**Function**

According to the National Institute of Standards and Technology's Computer Security Resource Center, 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 an 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* defines 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 program's effectiveness.

The *IG FISMA Reporting Metrics* align with the five function areas in the National Institute of Standards and Technology's, or NIST's, *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 to achieve specific cybersecurity outcomes and guidance to achieve those outcomes.

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

| Function area | Domain | Related *Cybersecurity Framework* categories |
|---|---|---|
| **Identify** | Risk Management | Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy |
| **Identify** | Supply Chain Risk Management | Supply Chain Risk Management |
| **Protect** | Configuration Management | Information Protection Processes and Procedures |
| **Protect** | Identity and Access Management | Identity Management and Access Control |
| **Protect** | Data Protection and Privacy | Data Security |
| **Protect** | Security Training | Awareness and Training |
| **Detect** | Information Security Continuous Monitoring | Security Continuous Monitoring |
| **Respond** | Incident Response | Response Planning, Communications, Analysis, Mitigation, and Improvements |
| **Recover** | Contingency Planning | Recovery Planning, Improvements, and Communications |

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

IGs are required to assess the effectiveness of agency information security programs on a maturity model spectrum in which the foundational levels ensure that agencies develop sound policies and procedures and 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 *IG FISMA Reporting Metrics* states that achieving Level 4, Managed and Measurable, or above represents an effective level of security. However, the *IG FISMA Reporting Metrics* provides that the OIGs have the discretion to determine that their respective 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, which include protecting the EPA's critical assets; information technology, or IT; and information management activities. The Office of Information Security and Privacy, within the Office of Mission Support, promotes agencywide cooperation in managing risks and protecting EPA information in alignment with mission objectives. It defines clear, comprehensive, and enterprisewide information security and privacy strategies, including the information security program's mission, vision, goals, objectives, and performance measures. Agency personnel stated that the Office of Mission Support allocates a subset of $25,474,806 of its overall budget to its IT Security and Privacy Program, which includes the Office of Information Security and Privacy.

## Scope and Methodology

We conducted this performance audit from April 2023 to April 2024 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.[1] 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 objective. 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 20 supplemental IG FISMA reporting metrics required for FY 2023. We assessed these 40 metrics to be at an overall maturity of Level 3, Consistently Implemented, for the domains within each FISMA security function area, which denotes that the Agency's policies, procedures, and strategies are consistently implemented but that quantitative and qualitative effectiveness measures are lacking. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. This resulted in 32, or 80 percent, of the 40 metrics for FY 2023 being assessed up to Level 4. We documented justifications for those metrics that were assessed at Level 4 but that did not result in a rating of Level 4.

We interviewed Agency personnel, reviewed relevant Agency IT 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 Water's Safe Drinking Water Information System to review. We assessed controls around the selected system for those metrics targeted at the system level.

We provided the Agency with our assessment of each function area of the FY 2023 IG metrics and discussed the results. On July 27, 2023, we submitted the *OIG Completed CyberScope Template* to the OMB, which is detailed in Appendix D and includes our assessment for each of the 40 FY 2023 IG metrics for FY 2023, and Appendix E displays the individual domain ratings..

## Prior Reports

We followed up on Recommendation 2 from EPA OIG Report No. 22-E-0028, *The EPA Lacks Documented Procedures for Detecting and Removing Unapproved Software on the Agency's Network*, issued

[1] An entity designs, implements, and operates internal controls to achieve its objectives related to operations, reporting, and compliance. The 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.

March 30, 2022. We recommended that the Agency develop and provide training on its processes for detecting and removing unapproved software to users with privileges to install software on the EPA's network. We verified that the Agency held the training and documented the attendees, and we consider this recommendation closed.

We also determined 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 not completed at the time of our audit. The estimated completion date in the Agency's tracking system has been updated to July 31, 2023.

EPA OIG Report No. 20-P-0120, *EPA Needs to Improve Its Risk Management and Incident Response Information Security Functions*, issued March 24, 2020, which documented the results of the FY 2019 EPA FISMA audit, included a recommendation for the EPA to develop and maintain an up-to-date inventory of software. Corrective action was completed for this recommendation in March 2020. Chapter 4 details our findings related to the Agency's IT asset inventory, which includes software.

# Chapter 2
# The EPA Needs to Develop and Update IT Documentation to Comply with Federal Requirements

We found that the Agency did not establish IT procedures related to the Supply Chain Risk Management domain, contrary to OMB requirements and NIST guidance. This occurred because the Agency lacked management oversight. We also found that the EPA failed to finalize a security training and awareness plan and that its *Information Security Continuous Monitoring Strategic Plan* needs to be updated to comply with NIST guidance. The absence of a finalized security training and awareness plan and of an updated *Information Security Continuous Monitoring Strategic Plan* occurred because the Agency did not prioritize updating these plans to comply with NIST guidance. Without IT documentation that complies with the latest federal standards, the Agency cannot ensure that the information security program is implementing the information system security controls needed to protect against internal and external risks.

## The EPA Failed to Establish Documented Procedures for Its Supply Chain Risk Management Processes

The EPA failed to establish documented procedures to ensure its compliance with NIST supply chain risk management guidance. NIST Special Publication, or SP, 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, updated as of December 10, 2020, includes a supply chain risk management family of controls that involves federal agencies developing, documenting, and implementing supply chain risk management processes and controls. Additionally, 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.

Agency personnel stated that the EPA developed the *Supply Chain Risk Management Strategic Plan* and a charter document to guide its supply chain risk management program. However, the charter does not document the procedures to address federal guidance for the Agency's supply chain risk management; rather, it establishes the responsibilities of its supply chain risk management Executive Board and the structure and frequency of its supply chain risk management meetings. The *Supply Chain Risk Management Strategic Plan* mentions three risk management tiers into which the plan should be integrated. However, it focuses only on the first tier and states that plans for the other two tiers are to be developed. Additionally, the *Supply Chain Risk Management Strategic Plan* states that the Executive Board will review progress on meeting the objectives outlined in the plan quarterly and will review and consider revisions to the plan itself periodically. However, since the plan's creation in September 2021, it has undergone just two updates: one in December 2021 and one in January 2022.

Neither the charter nor the strategic plan details procedures to facilitate the implementation of supply chain risk management controls to comply with NIST SP 800-53, Revision 5. The Agency lacked documented procedures because, while the Agency's Office of Information Security and Privacy usually

leads the effort to update the EPA's procedures documents for IT processes, the Office of Acquisition Solutions was tasked with creating the supply chain risk management enterprise-level procedures document. The Office of Acquisition Solutions' unfamiliarity with the Office of Mission Support's IT procedures development process, combined with a lack of management oversight, led to the delay in developing the supply chain risk management procedures document.

Without documented procedures specific to the Agency's supply chain risk management process, the Agency cannot ensure that its information security program adheres to NIST guidance for implementing the information system security controls needed to protect against supply chain risks.

## The EPA Did Not Finalize a Security Training and Awareness Plan

Our assessment of FY 2023 security training domain metrics found that the EPA did not finalize a security training and awareness plan. NIST SP 800-53, Revision 5, PM-14, "Testing, Training, and Monitoring," requires agencies to develop and maintain a process for conducting security and privacy training associated with their systems and to review those plans against their organizational risk management strategy.

The Agency did not finalize the plan because of competing priorities while it updates all its IT procedures. While the plan is not finalized and approved, Agency personnel stated that, at the time of this audit, a plan was being drafted and other documentation was being produced to support components of the security awareness strategy. However, without finalizing the security training and awareness plan, the Agency cannot ensure that the associated program is tailored to accomplish its mission and achieve its objectives.

## The EPA Needs to Update Its *Information Security Continuous Monitoring Strategic Plan*

The EPA has not updated its *Information Security Continuous Monitoring Strategic Plan* to comply with NIST guidelines. Specifically, NIST SP 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs*, dated May 2020, states that organizations implement information security continuous monitoring capabilities under the direction of an associated program. This program defines, establishes, implements, and operates the various aspects of information security continuous monitoring to provide the organization with the information necessary to make risk-based decisions regarding security statuses at all organizational risk management levels. The risk management levels consist of the organization, mission and business process, and system levels.

Agency personnel informed us that the Agency prioritized updating its IT documentation, including the *Information Security Continuous Monitoring Strategic Plan*, to comply with NIST SP 800-53, Revision 5, over other guidance, such as NIST SP 800-137A. This was done to ensure personnel used secure systems that comply with SP 800-53. However, Agency personnel also said that they did not have the resources to update its numerous IT procedures documents. For example, updates to the *Information Security Continuous Monitoring Strategic Plan* were neglected in favor of updating the IT procedures documents.

Without an updated *Information Security Continuous Monitoring Strategic Plan* that complies with the latest NIST standards and guidelines, the Agency could lack a mitigation process to make risk-based decisions regarding security statuses at all organizational risk management levels.

## Recommendations

We recommend that the assistant administrator for Mission Support:

1. Document supply chain risk management procedures to comply with National Institute of Standards and Technology Special Publication 800-53 guidance.

2. Finalize and distribute a security and awareness training plan to comply with National Institute of Standards and Technology Special Publication 800-53 guidance.

3. Update the *Information Security Continuous Monitoring Strategic Plan* to comply with National Institute of Standards and Technology Special Publication 800-137A guidance.

## Agency Response and OIG Assessment

The Office of Mission Support agreed with our recommendations and completed corrective actions for Recommendations 1 and 2. The Office of Mission Support stated that the supply chain management procedures and a security and awareness training plan to comply with NIST SP 800-53 guidance were documented. These corrective actions met the intent of Recommendations 1 and 2, which the Agency completed on November 21, 2023, and March 1, 2024, respectively. We consider these recommendations complete.

For Recommendation 3, the Office of Mission Support stated that it has made progress toward updating the *Information Security Continuous Monitoring Strategic Plan* to comply with NIST SP 800-137A guidance but has not completed these actions and revised the estimated completion date to October 5, 2024. We consider Recommendation 3 is resolved with planned corrective action pending.

The Agency's response to the draft report is in Appendix F.

# Chapter 3
# The EPA Needs to Implement Processes on Its Network that Comply with Federal Requirements

We found that the Agency's implementation of information security processes did not comply with FY 2023 FISMA metrics for the Incident Response domain because the Agency has not fully implemented logging security events within the time frame required by the OMB. Additionally, under the Risk Management domain, we found that the Agency lacked an automated process for detecting unauthorized hardware on its network, as required by NIST. The EPA did not fulfill these mandates because of overarching technical issues and a lack of prioritizing compliance. If it does not log security events, the EPA cannot effectively detect, investigate, and remediate cyberthreats. And without a process to monitor its network for unauthorized hardware, the Agency may not detect unauthorized access and is vulnerable to exploitation.

## The EPA Needs to Fully Implement Event Logging Configurations to Comply with Federal Requirements

The EPA has not completed implementing Event Logging Tier 1, or EL1, Basic Requirements and Event Logging Tier 2, or EL2, Intermediate Requirements, on the Agency's network in accordance with federal mandates. OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, dated August 27, 2021, states that agencies must reach EL1 maturity within one year and EL2 maturity within 18 months of the date of the memorandum. To attain EL1, the Agency and all its components, including at the enterprise and system level, must fully meet logging requirements for the ten categories laid out by the OMB. These categories include user-behavior monitoring, event forwarding, and basic centralized access requirements. To attain EL2, the Agency must fully meet logging requirements for not only the EL1 categories but also four others, including inspection of encrypted data.

In November 2021, the Agency developed a plan to track its progress toward meeting the EL1 and EL2 requirements. The Agency provided documentation stating that it has achieved 92.0 percent of system-level data, or data related to Agency information systems, and 95.7 percent of enterprise-level data, or data related to the organization as a whole, toward its EL1 compliance. However, the EPA needs to log 100 percent of required data to comply with the OMB mandate. The Agency acknowledged that it must address the following overarching issues to reach EL1 and EL2 compliance:

- The vendor tool does not have the robust logging capability to meet the OMB logging requirements, and capabilities need to be developed to get logs from isolated systems in the enterprise network to link with the vendor tool.
- The EPA has laboratories with extremely sensitive systems that could be affected by the resource-intensive logging needed to meet OMB requirements.

- The Agency does not have access to or control of the FISMA systems' servers that are hosted or managed by external providers. Contract modifications will be required to comply with OMB Memorandum M-21-31.

Without implementing OMB event logging mandates, the EPA lacks compliant processes in the detection, investigation, and remediation of cyberthreats.

## The EPA Needs to Develop and Implement an Automated Process for Detecting Unauthorized Hardware on Its Network

The EPA has not developed or implemented an automated process for detecting unauthorized hardware on its network. NIST SP 800-53, Revision 5, CM-8, "System Component Inventory," provides that each agency should develop and document an inventory of system components on its network. To be consistent with NIST guidance, each agency must ensure that the inventory accurately reflects the system and includes all components within the system. The agency must review and update the inventory on a frequency that the organization defines and ensure that it detects the presence of unauthorized hardware on the agency's network. The EPA's configuration management IT procedures in CIO 2150.3-P-05.2, *Information Security – Configuration Management (CM) Procedure*, require the use of an "automated mechanism" that runs daily to detect unauthorized hardware on the network for moderate- and high-risk information systems.

**IT Asset**

NIST Interagency Report 7693, *Specification for Asset Identification 1.1*, dated June 2011, defines an asset as "anything that has value to an organization," including a computing device, an IT system, an IT network, software, and related piece of hardware. NIST SP 1800-5, *IT Asset Management*, dated September 2018, states that IT assets "include servers, desktops, laptops, and network appliances."

The EPA has not implemented an automated process to detect unauthorized hardware on its network because it did not prioritize establishing one. The reason for this was the multiple phases needed to complete configuration of these capabilities. Agency officials informed us that the EPA has obtained a tool with this functionality, but the tool needs to be configured with all available IT assets and related information. Once the configuration is complete, the tool can generate a baseline of authorized hardware to identify unknown and possibly unauthorized hardware. The tool can then provide the baseline to the Agency for further analysis.

The lack of an automated process for monitoring the Agency's network for unauthorized hardware leaves the Agency vulnerable to exploitation by unauthorized access to Agency data, which could go undetected.

## Recommendations

We recommend that the assistant administrator for Mission Support:

4. Complete the Agency's plan to fulfill Event Logging Tier 1 and Event Logging Tier 2 maturity requirements on the EPA network.

5. Develop and implement an automated process for detecting unauthorized hardware on the EPA network.

## Agency Response and OIG Assessment

The Office of Mission Support agreed with these recommendations and provided acceptable planned corrective actions and estimated milestone dates. We consider these recommendations resolved with corrective action pending.

For Recommendation 4, the Office of Mission Support stated that event logging requirements are among its top priorities and that it has made considerable progress toward full implementation of all logging requirements. The Agency provided an estimated completion date for the corrective actions for this recommendation of August 15, 2024. For Recommendation 5, the Office of Mission Support stated that it would continue to mature the Agency's configuration management database to detect unauthorized devices. The Agency provided an estimated completion date for the corrective actions for this recommendation of January 15, 2025.

The Agency's response to the draft report is in Appendix F.

# Chapter 4
# The EPA Needs to Develop Internal Controls to Protect Its Network

When we assessed the Agency's risk management and configuration management metrics, we found that the EPA lacked the internal controls, as provided in NIST guidance and CIO directives, to:

- Verify the completeness and accuracy of the Agency's IT asset inventory.
- Remediate compliance findings with respect to information system configuration.
- Verify the accuracy of information systems' security objective risk levels in the Agency's Risk Management Framework, or RMF, tool per NIST standards.

Agency personnel stated that, while the Agency previously established internal controls to distribute reports from its scanning tool to system owners to communicate configuration compliance findings, it discontinued that practice after the system owners stated that the reports were too frequent and unnecessary. Because of this, the Agency cannot ensure that its system configurations comply with the established baselines. Additionally, the Agency did not have a process for reconciliation of IT assets against its RMF tool data. As a result, the Agency lacks accountability for and visibility of its information system components. Finally, inaccurate risk categorization levels could cause the EPA to submit inaccurate data to the OMB and to erroneously assess whether its systems comply with federal requirements because different risk levels are subject to different requirements.

**RMF Tool**

The Agency's RMF tool allows the collection and storage of RMF documentation and artifacts, as well as the tracking of data related to artifacts and authorizations, including signatures, titles, and other pertinent information. It facilitates continuous compliance monitoring and ongoing authorization for the Agency's IT systems.

## The EPA Needs to Develop and Implement a Process to Verify the Completeness and Accuracy of Its IT Asset Inventories

The EPA has not developed a process to validate and verify the completeness and accuracy of its IT asset inventories. NIST SP 800-53, Revision 5, CM-8, "System Component Inventory," provides that each agency should develop and document an inventory of system components that accurately reflects the system and includes all components within the system. Additionally, it provides that each agency review and update the inventory on a frequency that the organization defines. Agency configuration management IT procedures in CIO 2150.3-P-05.2 state that the EPA must develop, document, and maintain an inventory of information system components that, among other requirements, accurately reflects the information system. CIO 2150.3-P-05.2 further provides that the EPA must "[r]eview and update the system component inventory annually or when authorized changes are made." Updating the

inventory of IT assets, which includes all an information system's components, is an integral part of the component installations, removals, and information system updates. OIG Report No. 20-P-0120 recommended that the Agency develop and maintain an up-to-date inventory of its software, which is a part of its IT assets. Corrective actions to address that recommendation were completed upon the issuance of that report on March 24, 2020.

**System Component**

NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, defines a system component as a "discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware."

Agency personnel stated that quarterly reports of IT assets are submitted to the OMB in response to chief information officer FISMA data calls. However, the EPA has not established a process to reconcile all IT assets between the Agency's registry of applications and its RMF tool, which houses all FISMA-related documentation. This is due to the Agency focusing its efforts on the specific metrics requested by the OMB in the quarterly submissions and not on all EPA information systems and accompanying IT asset inventories. While the EPA has established a process for information security officers to attest to all IT assets in their purview via an annual IT asset certification, this process began in August 2023, after our CyberScope responses were submitted to the OMB.

Without the verification of a complete and accurate inventory of IT assets, the Agency lacks accountability for and visibility of information system components on its network.

## The EPA Needs to Develop and Implement a Process for Monitoring and Remediating Configuration Compliance Findings

Relevant Agency personnel are not monitoring and remediating the EPA information systems' configuration compliance findings. Configuration compliance findings relate to changes to the baseline configuration of a system or IT asset that make the configuration no longer comply with Agency or federal requirements. For example, a system's password expiration setting could initially be configured to 90 days; however, as requirements change, the password expiration requirement could be updated to 45 days. In this case, if the system's baseline configuration remains at 90 days, it would incur a configuration compliance finding for not being set at 45 days. Agency configuration management IT procedures in CIO 2150.3-P-05.2 state that security information officers, information security officers, and EPA system owners or their official designees for EPA-operated systems must develop, document, and maintain baseline configurations under configuration control for the information system. CIO 2150.3-P-05.2 further provides that the EPA must review and update the baseline configuration of the system annually, when significant changes are made to the system, and when system components are installed or upgraded.

**Baseline Configuration**

NIST SP 800-171, defines a baseline configuration as a "documented set of specifications that has been formally reviewed and agreed upon at a given point in time."

The Agency has not established a process for monitoring and remediating configuration compliance findings by the information system officers and system owners. This is because recipients of previously distributed reports of configuration compliance findings from the Agency's scanning tool stated that they found the reports too frequent and unnecessary. Based on that feedback, the Agency chose to distribute configuration compliance findings only when requested. The EPA is working with the contractors responsible for the government's Cybersecurity and Infrastructure Security Agency Continuous Diagnostics and Mitigation dashboard to include configuration compliance finding data for the EPA's users. However, Agency personnel stated that an upgrade of the EPA's Continuous Diagnostics and Mitigation dashboard software, as well as in the time needed by contractor support to implement these requested features for the EPA, delayed progress.

Without consistent monitoring and remediation of compliance findings, the Agency cannot ensure that systems are configured to meet the established baseline, potentially exposing the EPA's information systems to security risks and compliance issues, which can affect the quality, reliability, and efficiency of its IT performance.

## The EPA Needs to Develop and Implement a Process to Verify the Accuracy of Information System Security Objective Risk Categorization Levels in Its RMF Tool

We found that the confidentiality, integrity, and availability categorization levels recorded in the Agency's RMF tool did not always match those documented in the associated systems' security plans. NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*, dated December 2018, provides that agencies should (1) develop and implement an organization wide strategy for continuously monitoring control effectiveness, (2) allocate security and privacy requirements to the system and to the environment of operation, (3) register the system with organizational program or management offices, and (4) document the characteristics of the system and the controls for the system and environment of operation in security and privacy plans.

**Loss of Confidentiality, Integrity, and Availability**

A loss of confidentiality is the unauthorized disclosure of information.
A loss of integrity is the unauthorized modification or destruction of information.
A loss of availability is the disruption of access to or use of information or an information system.

Source: NIST Federal Information Processing Standards Publication 199

NIST Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated February 2004, establishes security categories of confidentiality, integrity, and availability that a federal information system must use to determine the

overall security category of the system. In addition, NIST SP 800-37, Revision 2, provides that security categorization information "is documented in the system security plan."

Agency personnel stated that confidentiality, integrity, and availability categories for systems are categorized in accordance with NIST guidelines. However, these categorizations are recorded in the systems' security plans, usually as a word processing or PDF document and as attributes recorded in the Agency's RMF tool. The two sources of data do not automatically reconcile changes made to the categorization information. Inaccurate risk categorization levels in the Agency's RMF tool could lead to erroneous data being submitted to the OMB and an inconsistent assessment of Agency systems for federal compliance because of differing requirements for systems of higher risk.

## Recommendations

We recommend that the assistant administrator for Mission Support:

6. Develop and implement internal controls to validate the EPA's registry of applications with Risk Management Framework tool data for asset inventory completeness and accuracy verification.

7. Develop and implement internal controls to verify the completeness and accuracy of the EPA's inventory of information system components.

8. Collaborate with system owners and other relevant 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.

9. Develop and implement internal controls to validate that all information security officers confirm that the confidentiality, integrity, and availability categorization levels documented in the system security plans for their systems accurately match the levels recorded in the Risk Management Framework tool.

## Agency Response and OIG Assessment

The Office of Mission Support agreed with our recommendations; completed corrective actions for Recommendations 6, 7 and 9; and provided acceptable planned corrective actions and an estimated milestone date for Recommendation 8, which we consider resolved with corrective action pending.

For Recommendation 6, the Office of Mission Support stated that its Office of Information Security and Privacy has conducted a data call to reconcile its registry of applications. The Office of Information Security and Privacy will perform this data call annually and require system stakeholders to perform reviews and validations of information system assets, such as hardware and software. These corrective actions met the intent of Recommendation 6, which the Agency completed on May 31, 2023. We consider this recommendation complete.

For Recommendations 7 and 9, the Office of Mission Support stated that it has implemented an annual System Inventory Methodology that includes requiring information security officers and system owners to digitally sign an "Authorization Boundary and System Classification" questionnaire to verify the completeness and accuracy of the EPA's inventory of information system components. These corrective actions met the intent of Recommendations 7 and 9, which the Agency completed on June 28, 2023. We consider these recommendations complete.

For Recommendation 8, OIG questioned the Agency's proposed corrective actions for the original recommendation from the draft report which pointed to information technology procedures that were already in place when the finding was identified. OMS personnel stated the original recommendation described actions the Agency is currently performing. Through conversation with Agency personnel, the OIG revised the recommendation to more directly address the root cause of the baseline configuration compliance findings and give the Agency the flexibility to determine how they will address them. In response to the revised recommendation, the Agency proposed acceptable corrective actions and estimated milestone dates. We consider this recommendation resolved with corrective actions pending.

The Agency's response to the draft report is in Appendix F.

# Status of Recommendations

| Rec. No. | Page No. | Recommendation | Status* | Action Official | Planned Completion Date |
|---|---|---|---|---|---|
| 1 | 8 | Document supply chain risk management procedures to comply with National Institute of Standards and Technology Special Publication 800-53 guidance. | C | Assistant Administrator for Mission Support | 11/21/23 |
| 2 | 8 | Finalize and distribute a security and awareness training plan to comply with National Institute of Standards and Technology Special Publication 800-53 guidance. | C | Assistant Administrator for Mission Support | 3/1/24 |
| 3 | 8 | Update the *Information Security Continuous Monitoring Strategic Plan* to comply with National Institute of Standards and Technology Special Publication 800-137A guidance. | R | Assistant Administrator for Mission Support | 10/15/24 |
| 4 | 11 | Complete the Agency's plan to fulfill Event Logging Tier 1 and Event Logging Tier 2 maturity requirements on the EPA network. | R | Assistant Administrator for Mission Support | 8/15/24 |
| 5 | 11 | Develop and implement an automated process for detecting unauthorized hardware on the EPA network. | R | Assistant Administrator for Mission Support | 1/15/25 |
| 6 | 15 | Develop and implement internal controls to validate the EPA's registry of applications with Risk Management Framework tool data for asset inventory completeness and accuracy verification. | C | Assistant Administrator for Mission Support | 5/31/24 |
| 7 | 15 | Develop and implement internal controls to verify the completeness and accuracy of the EPA's inventory of information system components. | C | Assistant Administrator for Mission Support | 6/28/23 |
| 8 | 15 | Collaborate with system owners and other relevant 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. | R | Assistant Administrator for Mission Support | 11/1/24 |
| 9 | 15 | Develop and implement internal controls to validate that all information security officers confirm that the confidentiality, integrity, and availability categorization levels documented in the system security plans for their systems accurately match the levels recorded in the Risk Management Framework tool. | C | Assistant Administrator for Mission Support | 6/28/23 |

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

## Appendix A

# *Key Definitions*

**Baseline Configuration:** NIST SP 800-171 defines a baseline configuration as a "documented set of specifications … that has been formally reviewed and agreed on at a given point in time."

**Function:** NIST's Computer Security Resource Center glossary defines a function as "[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 functions are Identify, Protect, Detect, Respond, and Recover."

**IT Asset:** NIST Interagency Report 7693 defines an asset as "anything that has value to an organization," including a computing device, an IT system, an IT network, software, and related piece of hardware. NIST SP 1800-5 states that IG "assets include servers, desktops, laptops, and network appliances."

**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.

**Risk Management Framework Tool:** The Agency's RMF tool allows collection and storage of risk management framework documentation and artifacts; tracking of data related to artifacts; and authorizations, including signature, titles, and other pertinent information. It facilitates continuous compliance monitoring and ongoing authorization for the Agency's IT systems.

**Security Program:** NIST SP 800-16 defines a security program as "a program established, implemented, and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated" in its IT systems.

**System Component:** NIST SP 800-171 defines a system component as a "discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware."

## Appendix B

# *FY 2023 Core IG FISMA Reporting Metrics*

The numbers in the table correlate to the 66 metrics in the *IG FISMA Reporting Metrics*. However, the table only details the 20 core metrics that IGs were required to assess for FY 2023.

| | |
|---|---|
| **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, Credential, 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 & 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?<br>• Encryption of data at rest<br>• Encryption of data in transit<br>• Limitation of transfer to removable media<br>• Sanitization of digital media prior to disposal or reuse |
| 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)

*Numbers correlate to the list of 66 total metrics. The 20 listed in this table are the core metrics for FY 2023.

## Appendix C

# *FY 2023 Supplemental IG FISMA Reporting Metrics*

The numbers in the table below correlate to the 66 metrics in the *IG FISMA Reporting Metrics*. However, the table only details the 20 supplemental metrics that IGs were required to assess for FY 2023.

| |
|---|
| **Risk Management** |
| 7. 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? |
| 8. To what extent has the organization ensured that plans of action and milestones (POA&Ms) are used for effectively mitigating security weaknesses? |
| 9. 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? |
| **Supply Chain Risk Management** |
| 12. 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? |
| 13. To what extent does the organization use SCRM policies and procedures to manage SCRM activities at all organizational tiers? |
| **Configuration Management** |
| 19. 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? |
| 22. To what extent has the organization adopted the Trusted Internet Connection (TIC) 3.0 program to assist in protecting its network? |
| 24. To what extent does the organization use a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet-accessible federal systems? |
| **Identity, Credential, and Access Management** |
| 26. 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? |
| 27. To what extent does the organization use a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities? |
| 29. 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? |
| 33. 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? |
| **Data Protection & Privacy** |
| 35. 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? |

| Security Training |
| --- |
| 41. 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? |
| 43. 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? |
| **Information Security Continuous Monitoring** |
| 48. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization? |
| **Incident Response** |
| 57. 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? |
| 58. To what extent does the organization use the following technology to support its incident response program?<br>• Web application protections, such as web application firewalls<br>• Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools<br>• Aggregation and analysis, such as security information and event management (SIEM) products<br>• Malware detection, such as antivirus and antispam software technologies<br>• Information management, such as data loss prevention<br>• File integrity and endpoint and server security tools |
| **Contingency Planning** |
| 60. 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? |
| 65. 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? |

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

## *OIG-Completed CyberScope Template*

For Official Use Only

# Inspector General

Section Report

2023

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 consistently implements policy, procedures, and strategies for all five information security function areas, which we have concluded effectively adheres to the "FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics." We assessed the effectiveness of the Agency's information security program at Level 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. This resulted in 32 of 40 in -scope metrics for FY 2023 tested up to Level 4. For those metrics that were assessed at Level 4 but not rated at 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: • Information security documentation – We found the following discrepancies with EPA documentation: o The EPA lacks documented supply chain risk management information technology procedures and a finalized Supply Chain Risk Management strategy. o The EPA lacks a finalized security training and awareness strategy/plan related to Metrics #42 and #43. o The EPA's information security continuous monitoring, or ISCM, program assessment plan needs to be updated to comply with National Institute of Standards and Technology Special Publication 800-137A, dated May 2020, and NIST SP 800-53 Revision 5, dated September 2020. o The EPA lacks incident response procedures for what constitutes a major incident or which major incident requires an After Action Report. • Compliant information security processes – We found noncompliant information technology processes related to the following: o An established process for detection of unauthorized hardware on the Agency's network related to Metric #2. o Event Logging Tier 1 logging requirements related to incident detection and analysis specified in Metric #54 Maturity Level 3 description have not been met. • Internal control weaknesses – In addition to the above deficiencies, we noted the following internal control weaknesses during the FY 2023 FISMA assessment: o The Agency has not consistently implemented a process for communicating and remediating configuration failures. o The Agency lacks a process to validate and verify the completeness and accuracy of its inventory. o The Confidentiality, Integrity, and Availability categorization levels recorded in the Agency's FISMA Risk Management Framework tool did not match those documented in the system security plans for seven (64 percent) of the 11 sampled systems.

## Function 1A: Identify - 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?

Consistently Implemented (Level 3)

Comments : See remarks in question 11.2.

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?

Defined (Level 2)

Comments : We noted that the Agency lacks a process to validate and verify the completeness and accuracy of its inventory and a method for detecting unauthorized devices attached to the network.

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?

Consistently Implemented (Level 3)

Comments : We noted that the Agency lacks an ISCM strategic plan updated to comply with NIST standards to ensure an established software asset monitoring process is implemented.

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?

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?

Defined (Level 2)

Comments : We noted that the Confidentiality, Integrity, and Availability categorization levels recorded in the Agency's FISMA Risk Management Framework tool did not match those documented in the system security plans for eight (73%) of the 11 sampled systems.

6 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?

7 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 : See remarks in question 11.2.

8 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 : See remarks in question 11.2.

9 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 : See remarks in question 11.2.

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?

Consistently Implemented (Level 3)

Comments : We noted that EPA personnel stated that the Agency has not implemented the use of automated tools to perform scenario analysis and response modeling of a potential threat.

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 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications.

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

12 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 EPA lacks a finalized Supply Chain Risk Management strategy that has been communicated to personnel.

13 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 EPA lacks documented supply chain risk management procedures needed to meet the requirements of Metric #13.

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?

Ad Hoc (Level 1)

Comments : The EPA lacks documented supply chain risk management procedures needed to meet the requirements of Metric #14.

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

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

Ad Hoc (Level 1)

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 1 (Ad Hoc) 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.

Consistently Implemented (Level 3)

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 3 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 risk management program effective?

We assessed the effectiveness of the Agency's information security program at Level 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications.

## Function 2A: Protect - Configuration Management

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 contractoroperated systems?

19 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 : We noted that a process for communicating and remediating configuration failures is not consistently implemented.

20 To what extent does the organization use configuration settings/common secure configurations for its information systems?

Defined (Level 2)

Comments : We noted that a process for communicating and remediating configuration failures is not consistently implemented.

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?

Consistently Implemented (Level 3)

Comments : See remarks in question 25.2.

22 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network?

Defined (Level 2)

Comments : See remarks in question 25.2.

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, asappropriate?

24 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 : See remarks in question 25.2.

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

Defined (Level 2)

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 Configuration Management was Level 2 (Defined) based on a 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 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications.

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

26 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 : See remarks in question 34.2.

27 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 : See remarks in question 34.2.

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?

29 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 : See remarks in question 34.2.

30 To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDOor web authentication) for non- privileged users to access the organization`s facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

Consistently Implemented (Level 3)

Comments : See remarks in question 34.2.

31

To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDOor web authentication) for privileged users to access the organization`s facilities [organization-defined entry/exit points], networks, and systems, including for remote access?

Consistently Implemented (Level 3)

Comments : See remarks in question 34.2.

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?

Consistently Implemented (Level 3)

Comments : We noted that the Agency has not met the Event Logging Level 2 logging requirements specified for maturity Level 4 of Metric #32.

33 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 accesssessions?

Managed and Measurable (Level 4)

Comments : See remarks in question 34.2.

34.1 Please provide the assessed maturity level for the agency's Protect - Identity and Access 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 Identity, Credential, and Access Management was Level 3 based on Calculated Average for Identity, Credential, 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 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications.

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

35 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 : See remarks in question 40.2.

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?<br> Encryption of data at rest<br> Encryption of data in transit<br> Limitation of transfer to removable media<br> Sanitization of digital media prior to disposal or reuse

Managed and Measurable (Level 4)

Comments : See remarks in question 40.2.

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

Consistently Implemented (Level 3)

Comments : See remarks in question 40.2.

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 and E- Government Act of 20consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and userequirements)

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 (Managed and Measurable) 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 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications.

## Function 2D: Protect - Security Training

41 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 securityresponsibilities.

Managed and Measurable (Level 4)

Comments : See remarks in question 46.3.

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?

Consistently Implemented (Level 3)

Comments : We noted that the Agency lacks a finalized security awareness and training strategy or plan required by Metric #42, Maturity Level 3; therefore, we determined that this metric does not exceed Level 3.

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

Ad Hoc (Level 1)

Comments : We noted that the Agency does not have a finalized security awareness and training strategy or plan as required by the Maturity Level 2 and is therefore rated at Level 1 (Ad Hoc).

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)?

46.1 Please provide the assessed maturity level for the agency's Protect - Security Training 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 Security Training was Level 3 based on Calculated Average for Security Training Metrics Maturity calculations.

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

Consistently Implemented (Level 3)

Comments : Since the “FY 2023-2024 IG FISMA Reporting Metrics” requires inspectors general to determine function effectiveness by a calculated average model, we determined that the overall maturity of the Protect Function was Level 3 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 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications.

## Function 3: Detect - ISCM

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?

Consistently Implemented (Level 3)

Comments : See remarks in question 51.2.

48 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 : See remarks in question 51.2.

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?

Managed and Measurable (Level 4)

Comments : See remarks in question 51.2.

50 How mature is the organization`s process for collecting and analyzing ISCM performance measures and reporting findings?

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 domain ratings by a calculated average scoring model, we determined that the overall maturity of Information Security Continuous Monitoring was Level 4 based on Calculated Average for Information Security Continuous Monitoring 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 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications.

## Function 4: Respond - Incident Response

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?

54 How mature are the organization`s processes for incident detection and analysis?

Defined (Level 2)

Comments : While the EPA has tools and processes in place for incident detection and analysis, we noted that there are no established procedures for what constitutes a major incident or which major incident requires an After Action Report. Additionally, the Agency has not yet met the Event Logging Tier 1 logging requirements specified in Metric #54 for Maturity Level 3.

55 How mature are the organization`s processes for incident handling?

Managed and Measurable (Level 4)

Comments : See remarks in question 59.2.

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?

57 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 : See remarks in question 59.2.

58

To what extent does the organization use the following technology to support its incident response program?<br> Web application protections, such as web application firewalls<br> Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools<br> Aggregation and analysis, such as security information and event management (SIEM) products<br> Malware detection, such as antivirus and antispam software technologies<br> Information management, such as data loss prevention<br> File integrity and endpoint and serversecurity tools

Consistently Implemented (Level 3)

Comments : We noted that while the Agency has incident response technology processes in place, it lacks consistent, established processes to evaluate its incident response technologies.

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

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 Incident Response was Level 3 based on a Calculated Average for Incident Response Metrics Maturity.

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 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications.

## Function 5: Recover - Contingency Planning

60 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 : See remarks in question 66.2.

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

Consistently Implemented (Level 3)

Comments : See remarks in question 66.2.

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

63 To what extent does the organization perform tests/exercises of its information system contingency planning processes?

Consistently Implemented (Level 3)

Comments : We noted that the Agency was unable to provide documentation of contingency plan testing for 2021 for the sampled Safe Drinking Water Information System to fulfill the annual testing requirement, and the documentation provided for 2020 and 2022 did not provide test results.

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

65 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 teamsand used to make risk- based decisions?

Consistently Implemented (Level 3)

Comments : See remarks in question 66.2.

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

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 Contingency Planning was Level 3 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 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications.

## 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 | FY23 Assessed Maturity | FY23 Effectivness | Explanation |
|---|---|---|---|---|---|---|
| Identify | 2.33 | 3.00 | N/A | Consistently Implemented (Level 3) | Effective | We assessed the effectiveness of the Agency's information security program at Level 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Protect | 3.00 | 3.10 | N/A | Consistently Implemented (Level 3) | Effective | We assessed the effectiveness of the Agency's information security program at Level 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications. |
| Detect | 3.50 | 4.00 | N/A | Managed and Measurable (Level 4) | Effective | We assessed the effectiveness of the Agency's information security program at Level 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications. |
| | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Respond | 3.00 | 3.50 | N/A | Consistently Implemented (Level 3) | Effective | We assessed the effectiveness of the Agency's information security program at Level 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications. |
| Recover | 3.00 | 3.50 | N/A | Consistently Implemented (Level 3) | Effective | We assessed the effectiveness of the Agency's information security program at Level 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. For those metrics that were assessed at Level 4 but not rated at Level 4, we documented justifications. |

**The U.S. Environmental Protection Agency Office of Inspector General determined that, overall, the EPA has demonstrated that it consistently implements policy, procedures, and strategies for all five information security function areas, which we have concluded effectively adheres to the "FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics." We assessed the effectiveness of the Agency's information security program at Level 3. However, where support was provided and resources were allocated in a manner timely enough for the audit team to review, we assessed some metrics up to Level 4. This resulted in 32 of 40 in -scope metrics for FY 2023 tested up to Level**

| | | | | | | |
|---|---|---|---|---|---|---|
| **Overall Maturity** | **2.97** | **3.42** | **N/A** | **Consistently Implemented (Level 3)** | **Effective** | **4. For those metrics that were assessed at Level 4 but not rated at 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: • Information security documentation – We found the following discrepancies with EPA documentation: o The EPA lacks documented supply chain risk management information technology procedures and a finalized Supply Chain Risk Management strategy. o The EPA lacks a finalized security training and awareness strategy/plan related to Metrics #42 and #43. o The EPA's information security continuous monitoring, or ISCM, program** |

**assessment plan needs to be updated to comply with National Institute of Standards and Technology Special Publication 800-137A, dated May 2020, and NIST SP 800-53 Revision 5, dated September 2020. o The EPA lacks incident response procedures for what constitutes a major incident or which major incident requires an After Action Report. • Compliant information security processes – We found noncompliant information technology processes related to the following: o An established process for detection of unauthorized hardware on the Agency's network related to Metric #2. o Event Logging Tier 1 logging requirements related to incident detection and analysis specified in Metric #54 Maturity Level 3 description have**

| | |
|---|---|
| | **not been met. • Internal control weaknesses – In addition to the above deficiencies, we noted the following internal control weaknesses during the FY 2023 FISMA assessment: o The Agency has not consistently implemented a process for communicating and remediating configuration failures. o The Agency lacks a process to validate and verify the completeness and accuracy of its inventory. o The Confidentiality, Integrity, and Availability categorization levels recorded in the Agency's FISMA Risk Management Framework tool did not match those documented in the system security plans for seven (64 percent) of the 11 sampled systems.** |

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

| Maturity Level | Core | Supplemental |
|---|---|---|
| Ad Hoc (Level 1) | 0 | 0 |
| Defined (Level 2) | 2 | 0 |
| Consistently Implemented (Level 3) | 3 | 0 |
| Managed and Measurable (Level 4) | 0 | 3 |
| Optimized (Level 5) | 0 | 0 |
| **Calculated Rating:** | **2.60** | **4.00** |

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

| Maturity Level | Core | Supplemental |
|---|---|---|
| Ad Hoc (Level 1) | 1 | 1 |
| Defined (Level 2) | 0 | 1 |
| Consistently Implemented (Level 3) | 0 | 0 |
| Managed and Measurable (Level 4) | 0 | 0 |
| Optimized (Level 5) | 0 | 0 |
| **Calculated Rating:** | **1.00** | **1.50** |

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

| Maturity Level | Core | Supplemental |
|---|---|---|

| | | |
|---|---|---|
| Ad Hoc (Level 1) | 0 | 0 |
| Defined (Level 2) | 1 | 2 |
| Consistently Implemented (Level 3) | 1 | 1 |
| Managed and Measurable (Level 4) | 0 | 0 |
| Optimized (Level 5) | 0 | 0 |
| **Calculated Rating:** | **2.50** | **2.33** |

**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) | 3 | 1 |
| Managed and Measurable (Level 4) | 0 | 3 |
| Optimized (Level 5) | 0 | 0 |
| **Calculated Rating:** | **3.00** | **3.75** |

**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) | 1 | 0 |
| Managed and Measurable (Level 4) | 1 | 1 |
| Optimized (Level 5) | 0 | 0 |
| **Calculated Rating:** | **3.50** | **4.00** |

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

| Maturity Level | Core | Supplemental |
|---|---|---|
| Ad Hoc (Level 1) | 0 | 1 |
| Defined (Level 2) | 0 | 0 |
| Consistently Implemented (Level 3) | 1 | 0 |
| Managed and Measurable (Level 4) | 0 | 1 |
| Optimized (Level 5) | 0 | 0 |
| **Calculated Rating:** | **3.00** | **2.50** |

**Function 3: Detect - ISCM**

| 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) | 1 | 1 |
| Optimized (Level 5) | 0 | 0 |
| **Calculated Rating:** | **3.50** | **4.00** |

**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 | 1 |
| Managed and Measurable (Level 4) | 1 | 1 |
| Optimized (Level 5) | 0 | 0 |
| **Calculated Rating:** | **3.00** | **3.50** |

**Function 5: Recover - Contingency Planning**

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

| | | |
|---|---|---|
| Managed and Measurable (Level 4) | 0 | 1 |
| Optimized (Level 5) | 0 | 0 |
| **Calculated Rating:** | **3.00** | **3.50** |

Appendix E

# EPA FY 2023 FISMA Compliance Results

**Table E-1: Maturity level of the EPA's information security function areas and domains**

| Security function | Security domain | OIG-assessed maturity level |
|---|---|---|
| Identify | Risk Management | Level 3: Consistently Implemented |
| Identify | Supply Chain Risk Management | Level 1: Ad Hoc |
| Protect | Configuration Management | Level 2: Defined |
| Protect | Identity and Access Management | Level 3: Consistently Implemented |
| 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 3: Consistently Implemented |
| Recover | Contingency Planning | Level 3: Consistently Implemented |

Source: OIG assessment results by security function and domain. (EPA OIG table)

**Table E-2. OIG assessment results overall for the EPA**

| | |
|---|---|
| **The EPA's overall maturity rating:** | **Level 3, Consistently Implemented** |

Source: OIG assessment of the EPA's overall maturity rating. (EPA OIG table)

# Agency Response to Draft Report

OFFICE OF MISSION SUPPORT
WASHINGTON, D.C. 20460

May 16, 2024

**MEMORANDUM**

**SUBJECT:** Response to the Office of Inspector General Draft Report, Project No. OA-FY23-0061, "*The EPA Needs to Develop and Implement Information Technology Processes to Comply with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2023*" dated April 17, 2024

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

VAUGHN NOGA
Digitally signed by VAUGHN NOGA
Date: 2024.05.16 14:09:24 -04'00'

**TO:** LaSharn Barnes, Director
Information Resources Management
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 all nine recommendations.

AGENCY'S RESPONSE TO DRAFT AUDIT RECOMMENDATIONS

**Agreements**

| No. | Recommendation | High-Level Corrective Action(s) | Est. Completion Date |
|---|---|---|---|
| 1 | Document supply chain risk management procedures to comply with National Institute of Standards and Technology SP 800-53 guidance. | Information Security – Supply Chain Risk Management (SR) Procedure (Directive No: CIO 2150-P-26.0) has been updated to comply with related NIST SP 800-53, Revision 5 SCRM controls.<br><br>(See attachment 1) | Completed |
| 2 | Finalize and distribute a security and awareness training plan to comply with National Institute of Standards and Technology SP 800-53 guidance. | The Cybersecurity and Privacy Awareness and Training Plan has been established to address IT roles and positions.<br><br>(See attachment 2) | Completed |
| 3 | Update the *Information Security Continuous Monitoring Strategic Plan* to comply with National Institute of Standards and Technology SP 800-137A guidance. | Update the *Information Security Continuous Monitoring Strategic Plan* to comply with National Institute of Standards and Technology SP 800-137A guidance.<br><br>The EPA agrees with this recommendation and has made progress towards updating our Information Security Continuous Monitoring Plan. | June 1, 2024 |
| 4 | Complete the Agency's plan to fulfill Event Logging Tier 1 and Event Logging Tier 2 maturity requirements on the EPA network. | Complete the Agency's plan to fulfill Event Logging Tier 1 and Event Logging Tier 2 maturity requirements on the EPA network.<br><br>The EPA agrees with this recommendation and has made considerable progress towards full implementation of all event logging requirements as outlined in OMB M-21-31. Event Logging requirements are among EPA's top priorities. | August 15, 2024 |
| 5 | Develop and implement an automated process for | Develop and implement an automated process for detecting | January 15, 2025 |

| | | | |
|---|---|---|---|
| | detecting unauthorized hardware on the EPA network. | unauthorized hardware on the EPA network.<br><br>EPA agrees with this recommendation and will continue to mature the governance structure of the Agency's configuration management database (CMDB) to ensure the detection of unauthorized devices, which are devices that are not assigned to a FISMA boundary. Assets without an assigned FISMA boundary will be labeled as "unauthorized". Phases 1-4 focus on leveraging techniques to address the existing population of "unauthorized" assets. Phase 5 is to operate in parallel with Phases 1-4 focusing on establishing a governance structure that ensures data elements critical to an accurate CMDB are collected and maintained throughout the system lifecycle. | |
| 6 | Develop and implement internal controls to validate the EPA's registry of applications with Risk Management Framework tool data for asset inventory completeness and accuracy verification. | Develop and implement internal controls to validate the EPA's registry of applications with Risk Management Framework tool data for asset inventory completeness and accuracy verification.<br><br>The EPA agrees with this recommendation. OISP conducted a data call in 2023 to reconcile the registry of applications and the information in the GRC tool. OISP will conduct this data call annually requiring system stakeholders to perform reviews and validations of information system assets (e.g., hardware and software) between | May 31, 2024 |

| | | | |
|---|---|---|---|
| | | the registry of applications and the RMF tool. OISP will perform a compliance and oversight review to confirm completeness and accuracy. | |
| 7 | Develop and implement internal controls to verify the completeness and accuracy of the EPA's inventory of information system components. | EPA has implemented internal controls to verify the completeness and accuracy of the EPA's inventory of information system components. As part of the annual System Inventory Methodology the Information Security Officer (ISO) and System Owner (SO) are required to digitally sign an 'Authorization Boundary and System Classification' questionnaire. This is indicated in the System Inventory Methodology v1.0 document. OISP performs compliance and oversight reviews to confirm completeness and accuracy of the inventory.<br><br>(See Attachments 3-6) | Completed |
| 8 | Develop and implement a process for monitoring and remediating baseline configuration compliance findings, such as a process or documented procedures for system owners or information security officers to regularly review relevant data on the Continuous Diagnostics and Mitigation dashboard. | EPA has implemented the procedures listed below that establish a process for monitoring and remediating baseline configuration compliance findings.<br><br>• Information Security – Configuration Management (CM) Procedure (Directive No: CIO 2150.3-P-05.2, Dated June 2023)<br><br>• Information Security – Risk Assessment (RA) Procedure (Directive No: CIO 2150-P-14.3, Dated December 2023) | Completed |

| | | | |
|---|---|---|---|
| | | • Information Security – System and Information Integrity (SI) Procedure (Directive No: CIO 2150-P-17.3, Dated November 2023)<br><br>A Roles and Responsibility document (Directive No: CIO-2150.3-P-19.2, Dated May 2022) assigns responsibility for maintaining baseline configurations. Additionally, OISP has published a Plan of Action & Milestone (POA&M) Guide that assists users in creating, updating and completing POAM items in the Agency GRC tool.<br><br>(See attachments 7-11) | |
| 9 | Develop and implement internal controls to validate that all information security officers confirm that the confidentiality, integrity, and availability categorization levels documented in the system security plans for their systems accurately match the levels recorded in the Risk Management Framework tool. | EPA has implemented internal controls to verify the accuracy of system security categorizations. The EPA annual 'System Inventory Methodology' includes a memo from the SIO attesting that all system categorizations for their area of responsibility are accurate. The OISP performs compliance and oversight reviews of the R/POs system inventories and the SIO attestation memos. The inaugural Inventory Methodology was established and implemented in FY 2023.<br><br>(See Attachments 3-6) | Completed |

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.

cc:
LaSharn Barnes
Jeremy Sigel
LaVonda Harris
Eric Jackson Jr.
Sabrena Richardson
Erin Collard
David Alvarado
Austin Henderson
Tonya Manning
Mark Bacharach
Lee Kelly
Kaitlyn Khan
Yulia Kalikhman
Gregory Scott
Jan Jablonski
Marilyn Armstrong
Afreeka Wilson
Darryl Perez
OMS_Audit_Coordination
Susan Perkins
Andrew LeBlanc
Jose Kercado-Deleon

**ATTACHMENTS**

Attachment 1: Information Security Supply Chain Risk Management Procedure
Attachment 2: FY24 Agency-Wide Cybersecurity Training Plan – FINAL
Attachment 3: Authorization Boundary and System Classification Questionnaire
Attachment 4: HVA Questionnaire
Attachment 5: Inventory Review Memo Template
Attachment 6: SIO System Categorization Memo Template
Attachment 7: Information Security Configuration Management Procedure
Attachment 8: Information Security Risk Assessment Procedure
Attachment 9: Information Security System and Information Integrity Procedure
Attachment 10: Information: Information Security Roles and Responsibilities Procedures
Attachment 11: Xacta POA&M Guide v5.01 – Current March 2024

## Appendix G

# *Distribution*

The Administrator
Deputy Administrator
Chief of Staff, Office of the Administrator
Deputy Chief of Staff for Management, Office of the Administrator
Agency Follow-Up Official (the CFO)
Assistant Administrator for Mission Support
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
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 Workforce Solutions and Inclusive Excellence, 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
Office of Policy OIG Liaison
Office of Policy GAO Liaison
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 Inquiries:** OIG.CongressionalAffairs@epa.gov

**Media Inquiries:** OIG.PublicAffairs@epa.gov

**EPA OIG Hotline:** OIG.Hotline@epa.gov

**Web:** epaoig.gov

## Follow us:

**X (formerly Twitter):** @epaoig

**LinkedIn:** linkedin.com/company/epa-oig

**YouTube:** youtube.com/epaoig

**Instagram:** @epa.ig.on.ig

**www.epaoig.gov**