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.