25-P-0023
April 2, 2025

At a Glance

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

Why We Did This Audit

To accomplish this objective:

The U.S. Environmental Protection Agency Office of Inspector General conducted this audit to assess the EPA's compliance with the fiscal year 2024 Inspector General Federal Information Security Modernization Act of 2014 reporting metrics.

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

To support these EPA mission-related efforts:

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

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

List of OIG reports.

What We Found

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

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

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

Recommendations and Planned Agency Corrective Actions

We recommend that the assistant administrator for Mission Support:

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

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