Office of Inspector General
U.S. Environmental Protection Agency
At a Glance

23-E-0021
July 5, 2023

The EPA's Vulnerability Tracking and Remediation and Information Technology Procedures Review Processes Are Implemented Inconsistently

Why We Did This Evaluation

To accomplish this objective:

The U.S. Environmental Protection Agency Office of Inspector General conducted this evaluation to assess the EPA's compliance with the fiscal year 2022 inspector general reporting metrics for the Federal Information Security Modernization Act of 2014.

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 rate their agencies' information security programs:

- Level 1 (Ad Hoc).
- Level 2 (Defined).
- Level 3 (Consistently Implemented).
- Level 4 (Managed and Measurable).
- Level 5 (Optimized).

To support these EPA mission-related efforts:

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

To address this top EPA management challenge:

- *Protecting EPA systems and other critical infrastructure against cyberthreats.*

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 *FY 2022 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 has deficiencies in the following areas:

Without timely tracking and remediation of known vulnerabilities, the Agency risks compromising the confidentiality, integrity, and availability of environmental and radiation data used for determining responses to national incidents and safeguarding first responder personnel.

- Updating information security procedures in a timely manner to meet the requirements of National Institute of Standards and Technology publications within one year of their publication.
- Tracking and remediating vulnerabilities identified for the Analytical Radiation Data System in a timely manner.

Recommendations and Planned Agency Corrective Actions

We recommend that the assistant administrator for Mission Support develop a process to keep information security procedures consistent with the most current revision of the National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*. Additionally, we recommend that the assistant administrator for Air and Radiation develop, implement, and assign responsibilities for a plan to prioritize and schedule installation of patches that address critical vulnerabilities in the Analytical Radiation Data System within Agency required time frames. The Agency agreed with our recommendations and provided acceptable planned corrective actions with estimated milestone dates. We consider the recommendations resolved with corrective actions pending.