U.S. Environmental Protection Agency
Office of Inspector General

20-P-0120
March 24, 2020

At a Glance

Why We Did This Project

We performed this audit to assess the U.S. Environmental Protection Agency's compliance with the fiscal year 2019 Inspector General reporting instructions for the Federal Information Security Modernization Act of 2014.

The *FY 2019 IG FISMA Reporting Metrics* outlines five security function areas and eight corresponding domains to help federal agencies manage cybersecurity risks. The document also outlines five maturity levels by which IGs should rate agency information security programs:

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

This report addresses the following:

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

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

List of OIG reports.

EPA Needs to Improve Its Risk Management and Incident Response Information Security Functions

What We Found

Further implementation of risk management activities and incident response tools are needed to combat cybersecurity threats intended to steal and destroy confidential and sensitive information.

We assessed the maturity of the EPA's information security program at Level 3, *Consistently Implemented.* A Level 3 designation means that the EPA's policies, procedures, and strategies are consistently implemented but quantitative and qualitative effectiveness measures are lacking. To determine the EPA's maturity level, we reviewed the five security function areas outlined in the *FY 2019 IG FISMA Reporting Metrics:* Identify, Protect, Detect, Respond, and Recover. We also reviewed the eight corresponding domains: Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning.

While the EPA consistently implemented policies, procedures, and strategies for many of these function areas and domains, improvements are still needed:

- **Risk Management**: The EPA did not implement standard data elements for software and associated licenses used within the Agency's information technology environment, and the plans of action and milestones were not consistently used to mitigate security weaknesses.

- **Incident Response:** The EPA did not implement prescribed technologies to support its incident response program.

Appendix A contains the results of our FISMA assessment.

Recommendations and Planned Agency Corrective Actions

We recommend that the Assistant Administrator for Mission Support (1) develop and maintain an up-to-date inventory of Agency software and associated licenses, (2) establish a control to validate that Agency personnel are creating the required plans of action and milestones associated with vulnerability testing, and (3) implement prescribed technologies to support the EPA's incident response program.

The Agency concurred with our recommendations and provided acceptable corrective actions. All recommendations are considered resolved with planned corrective actions pending.