U.S. Environmental Protection Agency
Office of Inspector General

19-P-0058
January 30, 2019

At a Glance

Why We Did This Project

We conducted this audit to assess the U.S. Environmental Protection Agency's (EPA's) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) during fiscal year (FY) 2018.

The *Inspector General (IG) FISMA Reporting Metrics* document outlines five maturity levels for IGs to rate their agency's information security program:

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

We reported our audit results to the Office of Management and Budget (OMB). The OMB then calculates the overall maturity model level for each cybersecurity function within an agency's information security program.

This report addresses the following:

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

Send all inquiries to our public affairs office at (202) 566-2391 or visit www.epa.gov/oig.

Listing of OIG reports.

EPA Consistently Implements Processes Within Its Information Security Program, but Opportunities for Improvement Exist

What We Found

Further improvements are needed to strengthen internal processes to better protect human health and environmental data from cybersecurity threats.

The EPA has established an effective information security program for the five security functions and related domains defined in the *FY 2018 IG FISMA Reporting Metrics* and shown in the table below.

Security functions	Domains
Identify	Risk management
Protect	Configuration management, identity and access management, data protection and privacy, and security training
Detect	Information security continuous monitoring
Respond	Incident response
Recover	Contingency planning

Source: *FY 2018 IG FISMA Reporting Metrics*.

We concluded that the EPA has achieved an overall assessment of Maturity Level 3, which denotes that the agency consistently implements its policies, procedures and strategies within its information security program. However, the EPA can further improve its processes in the following domains to strengthen its information security posture:

- **Risk Management**—Implement standard data elements for hardware assets connected to the network and for software and associated licenses used within the agency's environment.
- **Security Training**—Implement a process for reporting on contractors' completion of role-based training.
- **Incident Response**—Implement certain technologies to support the incident response program.
- **Contingency Planning**—Implement a process to ensure that the results of business impact analyses are used to guide contingency planning efforts.

Appendix A contains the results of our assessments for the *FY 2018 IG FISMA Reporting Metrics*. We worked closely with EPA officials and, where appropriate, revised our assessments. We briefed the EPA on the results of our analyses. We made no recommendations based on our analyses, and the EPA agreed with our conclusions.