U.S. Environmental Protection Agency
Office of Inspector General

18-P-0031
October 30, 2017

At a Glance

Why We Did This Review

The Office of Inspector General 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) 2017.

The Inspector General (IG) FISMA reporting metrics outline five maturity levels for IGs to rate their agency's information security programs:

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

The maturity model is a tool that summarizes an agency's information security program and outlines activities to improve the program.

We reported our audit results using the CyberScope system developed by the U.S. Department of Homeland Security.

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's Information Security Program Is Established, but Improvements Are Needed to Strengthen Its Processes

What We Found

The EPA has an effective information security program and has completed all the requirements to achieve a Level 3 (Consistently Implemented) maturity level for the five security functions and related domains defined within the FY 2017 IG FISMA reporting metrics:

Although the EPA has an effective information security program, management emphasis is needed to achieve a higher level of maturity for the agency's information security program.

1. Identify – Risk Management.
2. Protect – Configuration Management, Identity and Access Management, and Security Training.
3. Detect – Information Security Continuous Monitoring.
4. Respond – Incident Response.
5. Recover – Contingency Planning.

We tested whether the EPA developed policies, procedures and strategies for each area within the IG FISMA reporting metrics. We also analyzed EPA management's self-assessments that contained assertions and additional information on whether the agency implemented processes and practices consistent with the specified security functions and related domains. In addition, we evaluated prior audit work to determine whether the self-assessments were consistent with our audit findings.

We concluded that the EPA defined policies, procedures and strategies for each security function and related domains. EPA management also provided sufficient evidence that the agency implemented a majority of processes and practices consistent with maturity model Level 3 (Consistently Implemented). However, we found substantial weaknesses in the EPA's information security training program related to how the agency verifies whether contractor personnel with significant information security responsibilities comply with specialized security training requirements.

Appendix A documents the results for the FY 2017 IG FISMA reporting metrics. We worked closely with EPA officials and briefed them on the results. We made no recommendations based on our analysis. The EPA agreed with our conclusions.