U.S. Environmental Protection Agency
Office of Inspector General

17-P-0044
November 14, 2016

At a Glance

Why We Did This Review

The Office of Inspector General (OIG) conducted this audit to evaluate the U.S. Environmental Protection Agency's (EPA's) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) during fiscal year 2016.

A robust but agile information security infrastructure is paramount to combat constant cybersecurity attacks. Security officials must understand the current status of their security programs and risk factors that could adversely affect organizational operations, assets, employees and external partnerships.

We reported our audit results using the CyberScope system developed by the Department of Homeland Security. CyberScope calculates the effectiveness of an agency's information security program based on the responses to the FISMA reporting metrics.

This report addresses the following EPA goal or cross-agency strategy:

- *Embracing EPA as a high-performing organization.*

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

Listing of OIG reports.

Improvements Needed in EPA's Information Security Program

What We Found

The EPA's information security function areas did not meet the defined requirements to be considered effective. We assessed the following five Cybersecurity Framework Function areas and the corresponding metric domains as specified by the fiscal year 2016 Inspector General FISMA reporting metrics.

More work is needed by the EPA to achieve managed and measurable information security function areas to manage cybersecurity risks.

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

We evaluated each security function area using the maturity model. The maturity model is a tool to summarize the status of an agency's information security program and to outline what still needs to be done to improve the program. The maturity model assesses each function area as: Level 1 - Ad-hoc, Level 2 - Defined, Level 3 - Consistently Implemented, Level 4 - Managed and Measurable, or Level 5 - Optimized.

The maturity model defines the requirements to meet a particular maturity level, and the EPA must meet all the requirements of that level before it can progress to the next higher level within the maturity model. The EPA would need to achieve Level 4 (Managed and Measurable) for a function area to be considered effective. The table below summarizes each function area the EPA achieved.

EPA's information security function area maturity

Security function areas	Maturity level rating
Identify, Protect, Respond, and Recover	Level 3 - Consistently Implemented
Detect	Level 2- Defined

Source: OIG testing results.

Appendix A contains the results for the fiscal year 2016 Inspector General FISMA reporting metrics.

We worked closely with EPA officials and briefed them on the results. Where appropriate, we updated our analysis and incorporated management's feedback. EPA agreed with our results. We made no recommendations based on our analysis.