U.S. Environmental Protection Agency
Office of Inspector General

17-P-0045
November 14, 2016

At a Glance

Why We Did This Review

The Office of Inspector General (OIG) performed this audit to document and selectively test the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) security practices related to performance measures, as outlined in the fiscal year 2016 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) reporting metrics, and to follow up on the status of prior-year audit recommendations.

FISMA requires the OIG to annually evaluate its respective agency's information security program designed to protect the operations and assets of the agency.

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 CSB goal:

- *Preserve the public trust by maintaining and improving organizational excellence.*

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

Listing of OIG reports.

CSB Has Effective "Identify" and "Recover" Information Security Functions, but Attention Is Needed in Other Information Security Function Areas

What We Found

More work is needed by CSB to achieve an overall managed and measurable information security program that can effectively manage cybersecurity risks.

Two of the five information security function areas at CSB are considered effective. We assessed the following five Cybersecurity Framework Security Function areas and the corresponding metric domains as specified by the fiscal year 2016 Inspector General FISMA reporting metrics:

1. Identify - Risk Management, Contractor System
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 CSB must meet all the requirements of that level before it can progress to the next higher level within the maturity model. The CSB 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 CSB achieved.

CSB's information security function area maturity

Security function areas	Maturity level rating
Identify and Recover	Level 5
Protect and Detect	Level 3
Respond	Level 2

Source: OIG testing results.

Additionally, CSB completed the 10 open recommendations from prior reports.

Appendix A contains the results for the fiscal year 2016 Inspector General FISMA reporting metrics. We met with CSB and updated our results based on additional information provided. CSB agreed with our results.