U.S. Environmental Protection Agency
Office of Inspector General

20-P-0077
February 12, 2020

At a Glance

CSB's Information Security Program Is Defined, but Improvements Needed in Risk Management, Identity and Access Management, and Incident Response

Why We Did This Project

We performed this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) compliance with performance measures outlined in the fiscal year (FY) 2019 Inspector General (IG) reporting instructions for the Federal Information Security Modernization Act of 2014 (FISMA).

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 CSB goal:

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

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

List of OIG reports.

What We Found

The CSB lacks documented procedures to address information technology risks and threats from cybersecurity incidents.

We assessed the maturity of the CSB's information security program at Level 2, *Defined*. A Level 2 designation means that the CSB's policies, procedures and strategies are formalized and documented but not consistently implemented. To determine the CSB's maturity level, we reviewed the five security function areas outlined in the *FY 2019 IG FISMA Reporting Metrics:* Identify, Protect, Detect, Respond and Recovery. 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 CSB has policies, procedures and strategies for many of these function areas and domains, improvements are still needed in:

- **Risk Management**—The CSB neither identified nor defined its procedures for identifying, assessing or managing supply chain risks for the agency's information systems.

- **Identity and Access Management**—The CSB lacks processes to allow users to access its systems with Personal Identity Verification cards. This issue was identified in a previous Office of Inspector General audit (Report No. 19-P-0147), and the CSB plans to complete corrective actions to resolve the deficiency by March 31, 2020.

- **Incident Response**—The CSB did not define incident handling processes specific to eradication in its incident response procedures.

Appendix A contains the results of our FISMA assessment.

Recommendations and Planned Agency Corrective Actions

We recommend that the CSB (1) define and document risk management procedures for identifying, assessing and managing supply chain risk and (2) define and document incident handling capabilities for the eradication of security incidents.

The CSB agreed with our recommendations and provided or completed acceptable corrective actions. Corrective action is pending for Recommendation 1 and complete for Recommendation 2.