U.S. Environmental Protection Agency
Office of Inspector General

19-P-0147
May 9, 2019

At a Glance

Why We Did This Project

We performed this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) security practices related to the performance measures outlined in the fiscal year (FY) 2018 Inspector General (IG) reporting metrics document for the Federal Information Security Modernization Act of 2014 (FISMA).

The *FY 2018 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.

CSB Still Needs to Improve Its "Incident Response" and "Identity and Access Management" Information Security Functions

What We Found

The CSB lacks established procedures for automated processes and authentication technologies, which could permit unauthorized access to agency systems.

We assessed the maturity of the CSB's information security program and determined it met the second of five levels: *Defined.* This means that policies, procedures and strategies are formalized and documented but not consistently implemented. While the CSB has policies, procedures and strategies for many of these function areas and domains, the agency still needs to improve the following issues that we previously identified in our FYs 2016 and 2017 FISMA audits:

- **Incident Response**—The CSB neither identified nor defined its incident response processes for incident handling, including the containment, eradication and recovery from incidents. The CSB did not document or formalize its rationale for not having an automated system to detect potential incidents. Additionally, the agency did not document established procedures to generate alerts based on log data analysis or record pertinent data of suspicious activity.

- **Identity and Access Management**—The CSB did not fully define or implement processes for the use of Personal Identity Verification cards for physical and logical access.

We also found that the CSB needs to make improvements to its "Data Protection and Privacy" domain, which was added to the *FY 2018 IG FISMA Reporting Metrics.* Appendix B contains the results of our FISMA assessments.

Recommendations and Planned CSB Corrective Actions

We recommend that the CSB improve its "Identity and Access Management," "Incident Response," and "Data Protection and Privacy" capabilities, including by implementing Personal Identity Verification card technology to strengthen access to its computers and network, and documenting its practices for data exfiltration and incident response. The CSB agreed with the five recommendations in this report and provided sufficient corrective actions and milestone dates for all of them. We consider the recommendations resolved with corrective actions pending.