U.S. Environmental Protection Agency
Office of Inspector General

16-P-0086
January 27, 2016

At a Glance

Why We Did This Review

The Office of Inspector General performed this audit to conduct a baseline assessment of the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) implementation of the information security policies and practices outlined by the 2015 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) reporting metrics.

FISMA requires federal agencies to develop an information security program that protects the operations and assets of the agency. The OIG performs an annual independent evaluation of the program.

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.

Fiscal Year 2015 Federal Information Security Modernization Act Report: Status of CSB's Information Security Program

What We Found

The effectiveness of the CSB's information security program is challenged by its lack of personal identity verification cards for logical access, complete system inventory, and documented policies and procedures for specialized security training.

We determined the CSB's baseline assessment of its information security areas using the criteria specified by the fiscal year 2015 Department of Homeland Security FISMA reporting metrics. This included collecting evidence of the existence of the CSB's policies and procedures, the CSB's self-assessment responses to the fiscal year 2015 FISMA metrics, and a discussion of CSB's control self-assessment with CSB management of selected information system security controls designated by the FISMA metrics. According to our control self-assessment results, the CSB information security program fully met the following FISMA metric sections:

- Continuous Monitoring Management.
- Configuration Management.
- Incident Response and Reporting.
- Risk Management.
- Plan of Action and Milestones.
- Remote Access Management.
- Contingency Planning.

For the remaining metrics, management attention is needed to improve processes that potentially could place these areas at risk.

- **Identity and Access Management.** CSB has not implemented the use of personal identification verification cards for logical access into its systems.
- **Security Training.** CSB does not have policies or procedures that specify the specialized training requirements for users with significant information security responsibilities.
- **Contractor Systems.** CSB lacks an inventory of systems operated on behalf of the agency, and does not have assurance that the security controls for those systems are effectively implemented.

Appendix A contains the U.S. Department of Homeland Security reporting metrics on the results of our analysis. CSB agreed with our results, and its complete response is in Appendix B.