U.S. Environmental Protection Agency
Office of Inspector General

16-P-0254
August 1, 2016

At a Glance

Why We Did This Review

We performed this audit to assess to what extent the U.S. Chemical Safety and Hazard Investigation Board (CSB) implemented information system security policies and procedures to protect CSB systems that provide access to national security or Personally Identifiable Information (PII) as outlined in Section 406 of the Cybersecurity Act of 2015.

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.

Cybersecurity Act of 2015 Report: CSB's Policies and Procedures to Protect Systems With Personally Identifiable Information

What We Found

Section 406 of the Cybersecurity Act of 2015 calls for Inspectors General of agencies with covered systems to report on several aspects of the covered systems' information system security controls. The term "covered system" means a national security system as defined in 40 U.S.C. § 11103 or a federal computer system that provides access to PII.

CSB has one system that contains sensitive PII. Safeguarding such information in the possession of the government and preventing its breach is essential to ensuring CSB retains the trust of the American public.

CSB identified one covered system that contains sensitive PII covered by provisions of the act. CSB does not have any national security information systems.

The act requires Inspectors General to report on the areas identified in the bullets below. We provided information in the following eight areas based on the requirements outlined in the act for CSB's covered system:

- Description of logical access policies and practices.
- Description of the logical access controls and multi-factor authentication used to govern privileged users access.
- Reasons for not using logical access controls and multi-factor authentication if applicable.
- Policies and procedures used to conduct inventories of software and licenses.
- Capabilities utilized to monitor and detect exfiltration and other threats.
- Description of how monitoring and detecting capabilities are utilized.
- Reasons why monitoring and detecting capabilities are not used if applicable.
- Description of policies and procedures used to ensure entities and contractors providing services to CSB are implementing the information security management practices identified in the act.

We worked closely with CSB throughout this audit to obtain the data in this report. We issued a draft report containing our conclusions, and subsequently briefed CSB representatives on the audit results. CSB agreed with our results, and did not provide a written response to this report.

The full version of this report contained controlled unclassified information. This is a redacted version of that report, which means the controlled unclassified information has been removed. The redactions are clearly identified in the report.