U.S. Environmental Protection Agency
Office of Inspector General

18-P-0030
October 30, 2017

At a Glance

Why We Did This Review

We performed this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) security practices related to performance measures outlined in the fiscal year 2017 Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA). The reporting metrics outline five maturity levels for IGs to rate their agency's information security programs:

Level 1 – Ad-Hoc
Level 2 – Defined
Level 3 – Consistently Implemented
Level 4 – Managed and Measurable
Level 5 – Optimized

We reported our audit results using the CyberScope system developed by the U.S. Department of Homeland Security, which calculates the effectiveness of the agency's information security 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.

Improvements Needed in CSB's Identity and Access Management and Incident Response Security Functions

What We Found

We rated CSB's information security program at Level 2 (Defined) for all five Cybersecurity Framework Security Function areas and corresponding metric domains assessed as specified by the fiscal year 2017 IG FISMA Reporting Metrics:

Weaknesses in the Identity and Access Management and Incident Response metric domains leave the CSB vulnerable to attacks occurring and not being detected in a timely manner.

1. Identify – Risk Management.
2. Protect – Configuration Management, Identity and Access Management, and Security Training.
3. Detect – Information Security Continuous Monitoring.
4. Respond – Incident Response.
5. Recover – Contingency Planning.

We tested whether the CSB developed policies, procedures and strategies for each area within the reporting metric. If the CSB developed policies, procedures and strategies consistent with the reporting metric question, we rated the agency at Level 2 (Defined).

We also conducted additional testing of CSB's patch management processes under the Configuration Management domain to determine whether the agency implemented the noted policies, procedures and strategies. We concluded that CSB's patch management processes graduated to a Level 5 (Optimized) maturity level rating.

While CSB has policies, procedures and strategies for many of the Cybersecurity Framework Security Function areas and corresponding metric domains, CSB lacks guidance and needs improvement in the following areas:

- **Identity and Access Management** – CSB does not include fully defined processes for Personal Identity Verification card technology for physical and logical access.

- **Incident Response** – CSB does not include fully defined incident response processes or technologies to respond to cybersecurity events.

Appendix A contains the results for the fiscal year 2017 IG FISMA Reporting Metrics. We worked closely with CSB throughout the audit to keep them apprised of our findings. We met with CSB on September 14, 2017, to brief them on our final results, and CSB agreed with our conclusions.