26-P-0042
June 14, 2026

At a Glance

Audit of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2025

Why This Audit Was Done

To accomplish this objective:

The U.S. Environmental Protection Agency Office of Inspector General contracted this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's compliance with the *Fiscal Year 2025 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*. We contracted with SB & Company LLC to perform this audit under our direction and oversight.

The *IG FISMA Reporting Metrics* outlines six security function areas and ten corresponding domains to help federal agencies manage cybersecurity risks. The document also outlines five maturity levels by which inspectors general should rate their agencies' information security programs:

Level 1, Ad Hoc.

Level 2, Defined.

Level 3, Consistently Implemented.

Level 4, Managed and Measurable.

Level 5, Optimized.

To support this CSB mission-related effort:

- *Creating and maintaining an engaged, high-performing workforce.*

Address inquiries to our public affairs office at 202-566-2391 or OIG.PublicAffairs@epa.gov.

List of OIG reports.

What SB & Company Found

SB & Company LLC concluded that the U.S. Chemical Safety and Hazard Investigation Board, also known as the CSB, achieved an overall maturity level of Level 2, Defined in fiscal year 2025. This means that the CSB's information security policies, procedures, and strategies are formalized and documented but not consistently implemented.

While the CSB maintained the same overall Level 2, Defined maturity level that it achieved in fiscal year 2024, SB & Company identified areas that need improvements associated with three *IG FISMA Reporting Metrics* domains: Risk and Asset Management, Identity and Access Management, and Contingency Planning. SB & Company concluded that the CSB does not have a documented process for regularly reviewing and validating the accuracy and completeness of its inventory or properly monitoring and tracking privileged user access, including the management of global administrator accounts. Additionally, the CSB did not require audit logs to be retained for a specified time frame to monitor and track user access and the historical usage of privileged accounts, nor did it conduct and document contingency plan tests or exercises completed on a regular, predefined schedule.

Without an accurate inventory, the CSB is at risk of not maintaining full visibility of its information technology assets and potential vulnerabilities, which may enable threat actors to compromise the network. Similarly, not properly monitoring privileged access and global administrator accounts increases the risk of unauthorized access to the CSB's data, and failure to retain sufficient access logs impairs breach detection capabilities. The absence of documented contingency plan tests or exercises also hampers vulnerability identification and staff preparedness, which can lead to a false sense of security.

The CSB needs improvements in the Risk and Asset Management, Identity and Access Management, and Contingency Planning domains related to its inventory, privileged user access, audit logs, and contingency plan testing.

Recommendations and Planned Agency Corrective Actions

SB & Company made four recommendations to the CSB, and the OIG agrees with and adopts the recommendations. The CSB concurred with SB & Company's recommendations, stating that it has completed the corrective actions for two recommendations; however, the CSB did not provide sufficient corrective action documentation to support closure of recommendations 1 and 4. The CSB provided acceptable planned corrective actions with estimated milestone dates for the remaining two recommendations. We consider all recommendations resolved with corrective actions pending.