



Office of Inspector General U.S. Environmental Protection Agency

At a Glance

22-E-0025
March 29, 2022

Why This Evaluation Was Done

This evaluation was performed to assess the U.S. Chemical Safety and Hazard Investigation Board's compliance with performance measures outlined in the fiscal year 2021 inspector general reporting instructions for the Federal Information Security Modernization Act of 2014.

SB & Company was contracted to perform this evaluation under the direction and oversight of the U.S. Environmental Protection Agency's Office of Inspector General.

The performance measures outline and provide potential ratings for security function areas to help federal agencies manage cybersecurity risks.

This evaluation supports the CSB mission-related effort:

- Preventing recurrence of significant chemical incidents through independent investigations.

Address inquiries to our public affairs office at (202) 566-2391 or OIG_WEBCOMMENTS@epa.gov.

[List of OIG reports.](#)

Contractor-Produced Report: CSB Is at Increased Risk of Losing Significant Data and Is Vulnerable to Exploitation

What SB & Company Found

SB & Company assessed the effectiveness of the CSB's information security program at "Level 2, Defined," which means that the CSB's policies, procedures, and strategies for its information security program are formalized and that its strategies are documented but not consistently implemented.

SB & Company found that the lack of off-site data backups increases the CSB's risk of losing significant data.

While the CSB has policies, procedures, and strategies in place for the information security program, SB & Company identified that the CSB lacks a Vulnerability Disclosure Policy to protect its public website. This increases the risk that vulnerabilities identified by external stakeholders are not being reported in a timely manner to CSB management. A delay in reporting identified vulnerabilities may increase the risk of exploitation of those vulnerabilities and lead to the disruption of operations.

SB & Company also identified that the CSB discontinued the off-site storage of tape backups, which increases the risk of losing data and disrupting operations. This issue was previously identified in OIG Report No. [21-E-0071](#), *CSB's Information Security Program Is Not Consistently Implemented; Improvements Are Needed to Address Four Weaknesses*, issued February 9, 2021. The CSB concurred with the recommendation in that report, implemented a corrective action, and restarted off-site backups. The CSB provided supporting documents for the corrective action taken, and we considered the corrective action for that recommendation completed. However, with the lack of on-site staff during the coronavirus pandemic, the CSB once again did not store backup tapes off-site. As a result, if the CSB headquarters loses data during an incident, those data could be permanently lost and impact the CSB's ability to fulfill its mission.

Recommendations and Planned Agency Corrective Actions

SB & Company made two recommendations to the CSB, and the OIG agrees with and adopts these recommendations. The CSB agreed with the recommendations and provided acceptable corrective actions. The OIG considers Recommendation 1 to be resolved with corrective action completed, and Recommendation 2 to be resolved with corrective action pending.