Office of Inspector General
U.S. Environmental Protection Agency
At a Glance

23-E-0016
May 2, 2023

Contractor-Produced Report: The CSB Is at Increased Risk of Losing Significant Data as Vulnerabilities Are Not Identified and Remediated Timely

Why This Evaluation Was Done

To accomplish this objective:

This evaluation was performed to assess the U.S. Chemical Safety and Hazard Investigation Board's compliance with the U.S. Department of Homeland Security's *Fiscal Year 2022 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.*

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

The reporting instructions outline five security function areas and nine 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:

- *Drive chemical safety change through independent investigations to protect people and the environment.*

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

List of OIG reports.

What SB & Company Found

The lack of vulnerability scans increases the risk that vulnerabilities are not identified and remediated in a timely manner and could result in data loss or disruption to Agency operations.

SB & Company concluded that the CSB achieved an overall maturity level of Level 1 (Ad-Hoc). This means that the CSB policies, procedures, and strategies are not formalized and activities are performed in an ad-hoc, reactive manner. While SB & Company assessed the effectiveness of the CSB's information security program at Level 2 (Defined), the *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* directs OIGs to consider specific core metrics when assigning the calculated maturity level for the CyberScope scoring. Because the core questions of the FY 2022 metrics were rated Level 1, the CSB's overall calculated maturity level resulted in a Level 1 CyberScope rating.

SB & Company also noted that the CSB discontinued the monthly vulnerability scans. This increases the risk that vulnerabilities are not identified and remediated timely and could result in data loss and disrupt the CSB's operations. This issue was previously identified in OIG Report No. 22-N-0058, *Management Alert: Data Vulnerabilities Could Impact the CSB's Ability to Carry Out Its Obligations Under the Federal Information Security Modernization Act of 2014 (Contractor-Produced Report),* issued September 22, 2022. The report summarized deficiencies SB & Company identified during the FY 2022 FISMA evaluation that required management's immediate attention, some of which were outside of the CyberScope questions. At the time of the evaluation, the CSB did not have a chief information officer or proper management oversight and, due to limited resources and staffing issues, the monthly vulnerability scans were discontinued. As a result, if the vulnerabilities are exploited in a cyberattack, the data could be permanently lost and impact the CSB's ability to fulfill its mission.

Recommendations and Planned Agency Corrective Actions

SB & Company made one recommendation to the CSB, and the OIG agrees with and adopts this recommendation. The CSB agreed with the recommendation and provided acceptable corrective actions. The OIG considers the corrective actions completed.