24-P-0035
April 29, 2024

# At a Glance

## *Contractor-Produced Report: The CSB Has Improved Its Information Security Program but Needs to Document Recovery Testing Results, Consistent with National Institute of Standards and Technology Guidelines*

### Why This Audit Was Performed

**To accomplish this objective:**

The U.S. Environmental Protection Agency Office of Inspector General conducted this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's compliance with the *FY 2023–2024 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 *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* outlines 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 goal:**

- *Advocating safety and achieving change through recommendations, outreach, and education.*

**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 concluded that the CSB achieved an overall maturity of Level 2, Defined, in fiscal year 2023. This means that the CSB's policies, procedures, and strategies are formalized and documented but not consistently implemented.

While the CSB has improved its overall maturity from the Level 1, Ad Hoc, rating it achieved in fiscal year 2022, SB & Company identified that improvements are still needed in the Incident Response domain within the Respond Function Area. Specifically, SB & Company concluded that the CSB should formally document the results of and the lessons learned during its disaster recovery testing scenarios. The National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, states that all recovery and reconstitution events should be well documented, including an after-action report with lessons learned. Because the CSB only has an informal process for documenting testing results and lessons learned, it did not fully document the results of its disaster recovery testing in a manner that was consistent with the National Institute of Standards and Technology guidelines.

**By formally documenting lessons learned and testing results, the CSB can strengthen its information security program's disaster recovery response times and mitigate the impacts of any disruptions.**

### 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 recommendation resolved with corrective actions pending.

### Noteworthy Achievements

The CSB hired a new chief information officer and deputy chief information officer in September 2022 and June 2023, respectively. These two officers have made significant progress in updating the CSB's information security program and addressing the concerns identified in fiscal year 2022 about the program's overall effectiveness. Specifically, the CSB established a strong working relationship with the Cybersecurity and Infrastructure Security Agency and enrolled in several of that agency's programs, including the Vulnerability Disclosure Program and the Continuous Diagnostics and Mitigation Program. The CSB also established a cloud presence, which it is now using to perform daily backups of critical servers to an off-site location.