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

July 14, 2026 | Report No. 26-P-0042

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

Abbreviations

CSB	U.S. Chemical Safety and Hazard Investigation Board
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
IG	Inspector General
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General

Cover Image

Image depicting network, data, and information security while highlighting the CSB's information security program for fiscal year 2025 rating of Level 2, Defined. Inspectors general rate the maturity level of their agencies' information security programs. The background is rows of coding and sketches. The foreground is a lock next to five bullets labeled Level 1, Ad Hoc; Level 2, Defined; Level 3, Consistently Implemented; Level 4, Managed and Measurable; and Level 5, Optimized.
(EPA OIG image and iStock.com/Allvisionn image as modified by OIG)

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, D.C. 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates.
Follow us on X @EPAoig.
Send us your Project Suggestions.

26-P-0042
July 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.

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

July 14, 2026

Mr. Steve Owens
Chairperson
U.S. Chemical Safety and Hazard Investigation Board
1750 Pennsylvania Avenue NW, Suite 910
Washington, D.C. 20006

Dear Mr. Owens:

This is a report on the U.S. Chemical Safety and Hazard Investigation Board's information security program. The report summarizes the results of the audit work performed by SB & Company LLC under the direction of the U.S. Environmental Protection Agency Office of Inspector General. This report also includes the SB & Company's completed fiscal year 2025 Federal Information Security Management Act reporting template, as prescribed by the Office of Management and Budget. The project number for this audit was OA-FY25-0042.

The report contains SB & Company's findings and recommendations. We agree with SB & Company's recommendations and adopt them as our own.

The CSB provided a response to SB & Company's recommendations, stating that corrective actions for recommendations 1 and 4 are completed; however, the CSB did not provide sufficient corrective action documentation to support closure of these recommendations. The CSB also provided acceptable planned corrective actions and estimated milestone dates in response to SB & Company's recommendations 2 and 3. All four recommendations are resolved with corrective actions pending.

The CSB is not required to respond to this report. If the CSB submits a response, however, it will be posted on the OIG's website, along with our memorandum commenting on the response. The response should be provided as an Adobe PDF file that complies with the requirements of section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that your office does not want released to the public; if the response contains such data, the CSB should identify the data for redaction or removal along with corresponding justification.

We will post this report to our website at www.epa.gov/oig.

Sincerely,

Nicole N. Murley

Nicole N. Murley
Deputy Inspector General
performing the duties of the Inspector General

Fiscal Year 2025 U.S. Chemical Safety and Hazard Investigation Board Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics

SB & Company, LLC

Table of Contents

Appendixes

SB & Company, LLC

Report of Independent Public Accountants

To the Management of the U.S. Chemical Safety and Hazard Investigation Board:

SB & Company LLC conducted a performance audit of the U.S. Chemical Safety and Hazard Investigation Board's, or the CSB's, compliance with the Federal Information Security Modernization Act, known as FISMA, for fiscal year 2025. The objective of this performance audit was to determine whether the CSB implemented an effective information security program. The scope of this audit was to assess the CSB's information security program consistent with FISMA and reporting instructions issued by the Office of Management and Budget and the Council of the Inspectors General on Integrity and Efficiency. The audit included tests of management, technical, and operation controls outlined in the National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, updated in December 2020.

For this audit, we reviewed the CSB's information technology systems. Our audit covered the CSB's headquarters located in Washington, D.C., from October 1, 2024, to June 15, 2025.

Our audit was performed in accordance with Generally Accepted Government Auditing Standards, as specified by the Government Accountability Office's Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We determined that the CSB's overall information security program is "Defined (Level 2)" because of the calculated average of the fiscal year 2025 FISMA core inspector general and fiscal year 2025 supplemental metrics. In our report, we have provided the CSB's acting chief information officer with four findings and four recommendations that, when addressed, should strengthen the CSB's information security program. The CSB's acting chief information officer agreed with our conclusion and recommendations (see Management Response, page 40).

Additional information on our findings and recommendations is included in the accompanying report.

SB & Company, LLC

Washington, D.C.
September 17, 2025

Background

Under the Federal Information Security Modernization Act of 2014, or FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.

Each fiscal year, the Office of Management and Budget issues an *IG FISMA Reporting Metrics* template for the inspector general of each federal agency to use to assess the agency's information security program. The *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*,[1] which can be found in Appendix A, provides 20 core and five supplemental metrics to be reviewed in FY 2025 across the ten function areas' domains. The supplemental metrics, as shown in Table 1, are assessed as to whether they provide sufficient data to determine, with a high level of confidence, the effectiveness of an Agency's information security program.[2] This Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks to critical infrastructure across the enterprise.

Table 1: *IG FISMA Reporting Metrics* and Cybersecurity Framework function areas, domains, and categories

Function Area	Domain	Related Cybersecurity Framework Categories
Govern	Cybersecurity Governance	Organizational Context, Risk Management Strategy, Roles, Responsibilities, and Authorities, Policy, and Oversight
Govern	Cybersecurity Supply Chain Risk Management	Cybersecurity Supply Chain Risk Management
Identify	Risk and Asset Management	Asset Management, Risk Assessment, and Risk Management Strategy
Protect	Configuration Management	Technology Infrastructure Resilience
Protect	Identity and Access Management	Identity Management, Authentication, and Access Control
Protect	Data Protection and Privacy	Data Security and Platform Security
Protect	Security Training	Awareness and Training
Detect	Information Security Continuous Monitoring	Continuous Monitoring and Adverse Event Analysis
Respond	Incident Response	Incident Management, Incident Analysis, Incident Response Reporting and Communication, and Incident Mitigation
Recover	Contingency Planning	Incident Recovery Plan Execution and Incident Recovery Communication

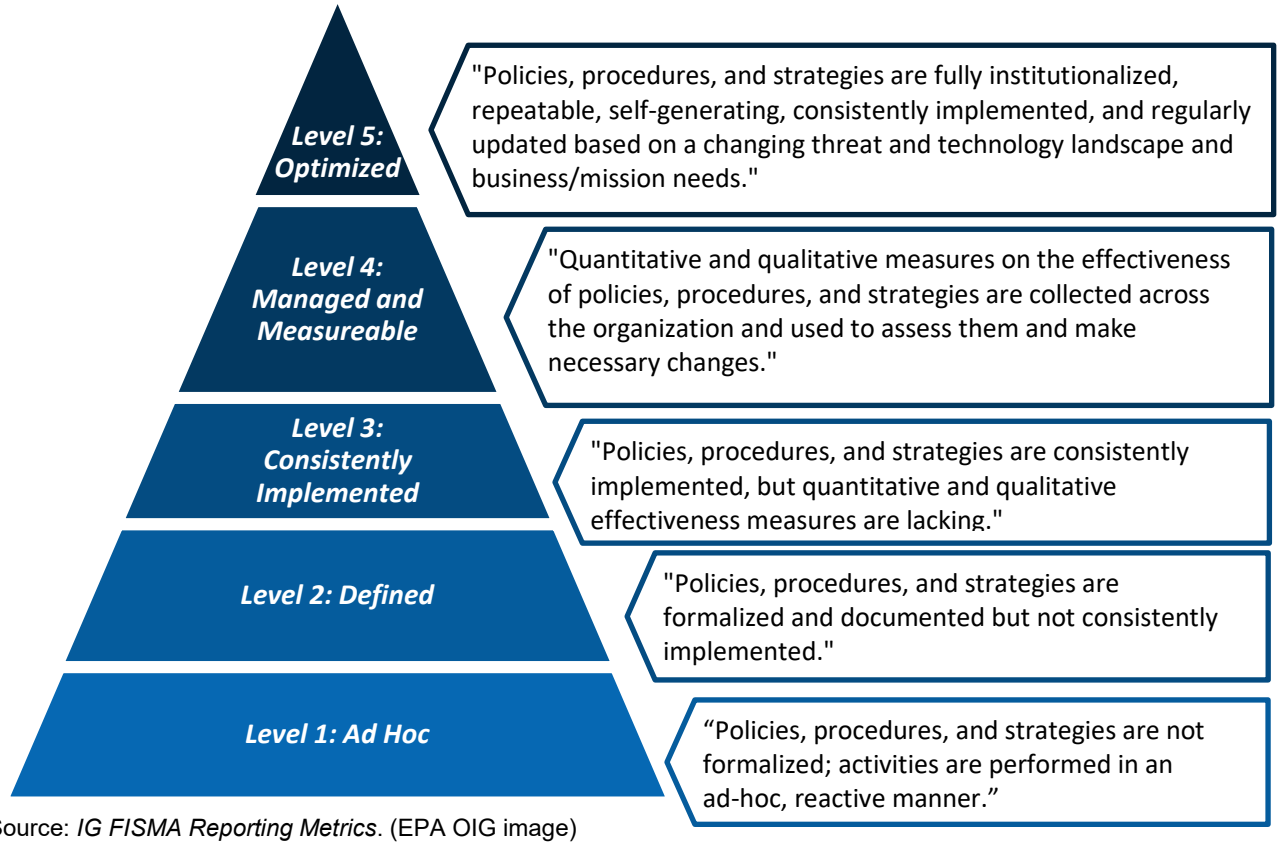
Source: *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 2.0, dated April 3, 2025 (EPA OIG table).

[1] *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*. These metrics were developed as a collaborative effort between the Office of Management and Budget and the Council of the Inspectors General on Integrity and Efficiency in consultation with stakeholders including the Federal Chief Information Officers Council.

[2] Executive Order 13636, Improving Critical Infrastructure Cybersecurity, was issued February 19, 2013, and directed the National Institute of Standards and Technology to develop a framework based on existing standards, guidelines, and practices to reduce cyber risks to critical infrastructure.

The effectiveness of an agency's information security program is based on a five-tiered maturity model spectrum, as shown in Figure 1. An agency's inspector general is responsible for annually assessing the agency's rating along this spectrum by determining whether the agency possesses the required policies, procedures, and strategies for each of the ten domains. The inspector general makes this determination by answering a series of questions about the domain-specific criteria that are presented in the annual *IG FISMA Reporting Metrics* template. An agency must fully satisfy each maturity level before it can be evaluated at the next maturity level. This approach requires the agency to develop the necessary policies, procedures, and strategies during the foundational levels (1 and 2). The advanced levels (3, 4, and 5) describe the extent to which the agencies have institutionalized those policies and procedures.

Figure 1: Maturity model spectrum



Source: *IG FISMA Reporting Metrics*. (EPA OIG image)

Scope and Methodology

SB & Company LLC, or we, conducted audit fieldwork from March to July 2025 in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Audit and applicable Government Auditing Standards, also known as the Yellow Book.

During our audit, we assessed whether the CSB exceeded maturity Level 2, Defined for each of the 35 questions for the ten domains in the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* and the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Metrics Evaluator's Guide*. We conducted a risk assessment of the *FY 2025 IG FISMA Reporting Metrics* to determine whether changes made to the underlying criteria of the FISMA metric questions had significantly changed since the FY 2024 audit.

We also evaluated the new FY 2025 criteria to assess whether they had significantly changed the CSB's responses to the overall metric questions since the FY 2024 audit. We assessed each new criterion as either:

- High Risk—The Office of Management and Budget introduced new reporting metrics, or the CSB made significant changes to its information security program since the FY 2024 audit for the identified metric question. or
- Low Risk—The CSB made no significant changes to its information security program since the FY 2024 audit for the identified metric question.

We relied on the responses to the FY 2024 CSB FISMA metric questions to answer the FY 2025 metric questions rated as *low risk*, and we conducted additional audit work to answer the questions rated as *high risk*.

We limited our assessment to determine whether the Agency possessed the noted policies, procedures, and strategies required for each metric under the function area based on the following criteria:

- If the policies, procedures and strategies were not formalized or documented, we rated the Agency at Level 1, Ad Hoc.
- If the policies, procedures, and strategies were formalized and documented, we rated the Agency at Level 2, Defined.
- If the Agency demonstrated that required security controls (such as access controls, incident response, and risk management) were implemented consistently, regular monitoring was performed, and staff received training on security policies and procedures, we rated the Agency at Level 3, Consistently Implemented.

We worked with and briefed the CSB on the audit results for each function area of the *FY 2025 IG FISMA Reporting Metrics.*

Appendix A provides the response to each FISMA metric, as submitted to the Office of Management and Budget by July 31, 2025, by the OIG.

Prior Audit

During our testing of the CSB's FY 2025 FISMA compliance, SB & Company LLC followed up on deficiencies identified in the FY 2024 FISMA audit, as documented in OIG Report No. 25-P-0037, *Audit of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024*, dated June 17, 2025. We reported that the CSB needed improvement associated with the reporting metrics' Identify domain in the Risk Management function area. We concluded that the CSB should ensure that its information can be reliably accessed in a timely manner even if key personnel are absent. Specifically, SB & Company LLC found that the CSB should: "Develop a process for designating and maintaining personnel in key roles (permanent and/or temporary) to ensure the continuity of essential security functions including the availability to respond to FISMA inquiries."

The CSB completed corrective actions for that recommendation. See Appendix B for more details on the status of corrective actions.

Results

The CSB's information security program is assessed overall at maturity Level 2, Defined. Table 2 specifies the maturity level for each function area and the associated domain.

Table 2: Maturity level of reviewed CSB function areas and domains

Function area	Domain	Overall OIG-assessed maturity level
Govern	Cybersecurity Governance	Level 2, Defined
Govern	Cybersecurity Supply Chain Risk Management	Level 2, Defined
Identify	Risk and Asset Management	Level 2, Defined
Protect	Configuration Management	Level 2, Defined
Protect	Identity and Access Management	Level 2, Defined
Protect	Data Protection and Privacy	Level 2, Defined
Protect	Security Training	Level 2, Defined
Detect	Information Security Continuous Monitoring	Level 2, Defined
Respond	Incident Response	Level 3, Consistently Implemented
Recover	Contingency Planning	Level 2, Defined

Source: *FY 2025 IG FISMA Reporting Metrics* and SB & Company LLC assessment. (SB & Company table)

However, in FY 2025, the CSB continues to need improvements in relation to specific questions in the Risk and Asset Management, Identity and Access Management, and Contingency Planning domains, as shown in Table 3.

Table 3: CSB domains that require further improvement

Function area	Domain	FISMA questions that need improvement
Identify	Risk and Asset Management	While the CSB has implemented asset management software, it does not have a documented process for regularly reviewing and validating the accuracy and completeness of its inventory. The absence of a complete inventory hinders effective cybersecurity risk management, as it prevents full visibility into potential vulnerabilities, unauthorized devices, and configuration compliance. Without an accurate inventory, it is difficult to enforce security controls, detect unauthorized changes, or respond effectively to security incidents. Additionally, without an accurate inventory, the CSB is at risk of not maintaining full visibility of its IT assets and potential vulnerabilities that may enable threat actors to compromise its network.
Protect	Identity and Access Management	While the CSB has a defined access management policy, it does not properly monitor and track privileged user access. Specifically, the CSB did not adequately manage access to global administrator accounts to ensure that privileged roles were appropriately granted or disabled when no longer needed. These accounts provide privileged users with the highest level of system access. Without proper monitoring of privileged access and global administrator accounts, the risk of unauthorized access to the CSB's data increases.
Protect	Identity and Access Management	While the CSB does retain user access logs, it did not provide evidence that sufficient audit logs are maintained for monitoring and tracking user access and the historical usage of privileged accounts. The current system only retains audit logs for 30 days. A failure to retain sufficient access logs impairs the CSB's breach detection capabilities.
Recover	Contingency Planning	While the CSB has defined policies, procedures, and processes for information system contingency plan testing and exercises, it does not conduct contingency plan tests or exercises on a regular, predefined schedule. Tests may be performed reactively rather than proactively to validate readiness. 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.

Source: SB & Company LLC assessment. (SB & Company LLC table)

The overall assessed level of the information security program was determined to be Level 2, Defined based on the calculated average of the individual metrics. The CSB continues to make significant progress in updating its cybersecurity program and ensuring that it upgrades security policies, tools, and practices as they evolve.

Conclusion

The U.S. Chemical Safety and Hazard Investigation Board's Information Technology Security Program has demonstrated that it has defined policies, procedures, and strategies for the Govern, Identify, Protect, Detect, and Recover information security function areas and consistently implemented these for the Respond function area. The U.S. Environmental Protection Agency Office of Inspector General contracted SB & Company LLC to assess the six cybersecurity framework function areas, and the contractor concluded that the CSB has achieved Level 2, Defined maturity, which denotes that the CSB has defined policies, procedures, and strategies in adherence to the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*. The CSB's Information Technology Security Program is considered not effective because, as provided in the *IG FISMA Reporting Metrics*, "OMB believes that achieving a Level 4 (managed and measurable) or above represents an effective level of security." While the CSB has policies, procedures, and strategies defined for these function areas and domains, improvements are needed in the overall Information Technology Security Program related to maintaining an accurate inventory, managing privilege user access and availability of audit logs, and regularly scheduled contingency plan testing.

The CSB would improve and strengthen its cybersecurity program by:

1. Developing a documented process for regularly reviewing and validating its inventory to ensure effective cybersecurity risk management and enforcement of security controls, detection of unauthorized changes, and responding effectively to security incidents.

2. Properly monitoring and tracking privileged user access, including the management of global administrator accounts.

3. Developing a procedure that requires audit logs to be retained for a specified time frame to monitor and track user access and the historical usage of privileged accounts.

4. Conducting and documenting that contingency plan tests or exercises are completed on a regular, predefined schedule.

Recommendations

We recommend that the chairperson for the U.S. Chemical Safety and Hazard Investigation Board:

1. Develop and implement a documented process to regularly review and validate the accuracy and completeness of the CSB's asset inventory, including both hardware and software.

2. Develop and implement a documented process for monitoring and tracking privileged user access, including the management of global administrator accounts from account creation to removal.

3. Develop and implement a procedure that requires audit logs to be retained for a specified time frame to monitor and track user access and the historical usage of privileged accounts.

4. Conduct and document that contingency plan tests or exercises are completed on a regular, predefined schedule.

CSB Responses and Procedures Performed

The CSB agrees with the notices of recommendation and has provided the following responses.

1. The CSB conducts an annual review of the agency's system inventory as outlined in the agency's management plan. This review supports cybersecurity risk management by validating asset records, identifying unauthorized changes, and ensuring alignment with security controls. While the process is documented internally, the materials provided to auditors did not clearly reflect the scope or structure of our inventory control system. The CSB is updating the agency's documentation to represent the review process and the agency's role more accurately in security enforcement.

2. The CSB is strengthening the agency's oversight of privileged user access, including the management of Global Administrator accounts. As part of this effort, the CSB is implementing procedures to monitor access assignments and changes within the Privileged Access Management System. This includes establishing a centralized mailbox to capture events such as the granting and revocation of user rights. These steps lay the foundation for broader access control strategy that supports accountability and security.

3. Building on the agency's access monitoring efforts, the CSB has implemented a mailbox-based system to retain privileged access logs for a period of three (3) years. This repository captures key events, including when users are granted or removed from privileged roles, and supports historical tracking, security investigations, and compliance review. The CSB is formalizing a procedure for this retention process to ensure audit log sufficiency and alignment with cybersecurity best practices.

4. The CSB is transitioning to a cloud-based infrastructure and, as part of this process, is developing a formal schedule for conducting contingency plan tests, including tabletop exercises and recovery validations. These tests will be tailored to reflect the CSB's operational structure and staffing levels, ensuring they are both practical and effective. The CSB will implement annual testing beginning January 2026, and the results will be reviewed to identify gaps and initiate corrective actions. This structured approach will strengthen the CSB's contingency planning and support operational resilience.

Status of Recommendations

Rec. No.	Page No.	Recommendation	Status*	Action Official	Planned Completion Date
1	8	Develop and implement a documented process to regularly review and validate the accuracy and completeness of the CSB's asset inventory, including both hardware and software.	R	Chairperson	9/20/25
2	8	Develop and implement a documented process for monitoring and tracking privileged user access, including the management of global administrator accounts from account creation to removal.	R	Chairperson	9/15/26
3	8	Develop and implement a procedure that requires audit logs to be retained for a specified time frame to monitor and track user access and the historical usage of privileged accounts.	R	Chairperson	9/15/26
4	8	Conduct and document that contingency plan tests or exercises are completed on a regular, predefined schedule.	R	Chairperson	4/20/26

* C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

Appendix A

SB & Company-Completed U.S. Department of Homeland Security CyberScope Template

This section shows the information uploaded to the U.S. Department of Homeland Security's Cyberscope program by the EPA OIG based on the template completed by SB & Company. The Cyberscope is the mechanism used to respond to the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

Inspector General

Section Report

2025

FISMA Annual IG

Chemical Safety Board

Function 0: Overall

0.1 Please provide an overall IG self-assessment rating (Effective/Not Effective)

Not Effective

Comments: Not Effective

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

The U.S. Chemical Safety and Hazard Investigation Board's Information Technology Security Program has demonstrated that it has defined policies, procedures, and strategies for the Govern, Identify, Protect, Detect and Recover information security function areas and consistently implemented for the Respond function Area. The U.S. Environmental Protection Agency Office of Inspector General contracted SB and Company LLC to assess the six Cybersecurity Framework function areas and the contractor concluded that the CSB has achieved a Level 2 (Defined) maturity, which denotes that the CSB has defined policies, procedures, and strategies in adherence to the FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0. The CSB's Information Technology Security Program is considered not effective. While the CSB has policies, procedures, and strategies defined for these function areas and domains, improvements are needed in the overall Information Technology Security Program related to managing privilege user access and availability of audit logs, maintaining an accurate inventory, and regularly scheduled contingency plan testing. The CSB should ensure that privileged user access is properly monitored and tracked and retain sufficient audit logs of individuals with system privileges. The CSB should also ensure the review and validation of its inventory of information systems for accuracy and completeness to align with its operational and security requirements. Additionally, the CSB should conduct contingency plan tests or exercises on a regular, predefined schedule.

Comments: The U.S. Chemical Safety and Hazard Investigation Board's Information Technology Security Program has demonstrated that it has defined policies, procedures and strategies for five of the six information security function areas and consistently implemented for the Respond Function Area. The U.S. Environmental Protection Agency Office of Inspector General contracted SB and Company LLC to assess the six Cybersecurity Framework function areas and concluded that the CSB has achieved a Level 2 (Defined) maturity, which denotes that the CSB has defined policies, procedures and strategies in adherence to the "FY 2024-2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics." The CSB's

Information Technology Security Program is considered not effective. While the CSB has policies, procedures, and strategies defined for these function areas and domains, improvements are still needed in the overall Information Technology Security Program related to managing privilege user access and availability of audit logs, maintaining an accurate inventory and regularly scheduled contingency plan testing. The CBS should ensure privilege user access is properly monitored and tracked and retain sufficient audit logs of individuals with system privileges. The CSB should also ensure the review and validation of its inventory of information systems for accuracy and completeness to align with its operational and security requirements. Additionally, the CSB should conduct contingency plan tests or exercises on a regular, predefined schedule.

Function 1A: Govern – Cybersecurity Governance

1. **FY25 Supplemental:** To what extent does the organization develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize and communicate its cybersecurity objectives?
[CG.01]
Defined (Level 2)

Comments: The CSB has defined its process for the development and maintenance of current and target cybersecurity profiles. However, the Agency did not use these target profiles to consider anticipated changes to the CSB's cybersecurity posture and does not assess the gaps between its current and target profiles to create and implement a prioritized action plan. Further, the CSB has not provided support that cybersecurity profiles are used to inform or align with broader strategic objectives, enterprise architecture, or investment decisions. This lack of provision limits their usefulness in assessing and communicating cybersecurity goals to internal and external stakeholders.

2. **FY25 Supplemental:** To what extent does the organization use a cybersecurity risk management strategy to support operational risk decisions?
[CG.02]
Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented its risk management strategy at the organizational, mission/business process, and system levels. The CSB consistently evaluates and adjusts its cybersecurity risk management strategy based on its threat environment and organizationwide cyber and privacy risk assessment. However, the CSB was not assessed beyond a Level 3 because the Agency lacks defined metrics to measure how effectively the cybersecurity risk management strategy influences operational risk decisions and it cannot validate whether the strategy is working as intended.

3. **FY25 Supplemental:** To what extent do cybersecurity roles, responsibilities, and authorities foster accountability, performance assessment, and continuous improvement?
[CG.03]
Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented and communicated an understanding of the roles, responsibilities, and authorities related to cybersecurity risk management. Significant cybersecurity duties are included in individuals' position descriptions and performance plans. While the CSB has established roles and responsibilities, the Agency was not assessed beyond a Level 3 because it does not use performance metrics to evaluate how effectively personnel execute their cybersecurity duties. This lack of measurement impedes accountability and improvement.

4.1 Please provide the assessed maturity level for the agency's Govern – Cybersecurity Governance program.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within Cybersecurity Governance, the domain is assessed as Level 2. We did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

4.2 Provide any additional information on the effectiveness (positive or negative) of the organization's cybersecurity governance program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the cybersecurity governance program effective?
[CG.SUM]
We assessed the effectiveness of the CSB's information security program at Defined (Level 2). For metrics assessed at Level 3 or below, we documented justifications for those ratings.

Function 1B: Govern – Cybersecurity Supply Chain Risk Management (C-SCRM)

5. **FY25 Core:** To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?
[C-SCRM.01]
Defined (Level 2)

Comments: The CSB has defined its policies, procedures, and processes for assessing and reviewing the supply chain- related risks associated with suppliers or contractors and the system. While the CSB has cybersecurity requirements in contracts, there is no formal process to track whether external providers are meeting all specified security or supply chain controls post-contract award. Due to the size of the CSB, the Agency only purchases hardware and software from Federal Risk and Authorization Management Program-approved vendors.

6.1 Please provide the assessed maturity level for the agency's Govern - Cybersecurity Supply Chain Risk Management (C-SCRM) program.
[GV.SUM]
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within Cybersecurity Supply Chain Risk Management, the domain is assessed as Level 2. We did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

6.2 Please provide the assessed maturity level for the agency's Govern program.
Defined (Level 2)

Comments: The maturity level for the Govern function is based on a calculated average of the individual metrics. We determined that the overall maturity for the Govern function is at Level 2.

6.3 Provide any additional information on the effectiveness (positive or negative) of the organization's supply chain risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the supply chain risk management program effective? [C-SCRM.SUM]

We assessed the effectiveness of the CSB's information security program at Defined (Level 2). For metrics assessed at Level 3 or below, we documented justifications for those ratings.

Function 2: Identify – Risk and Asset Management (RAM)

7. **FY25 Core:** To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections?
[RAM.01]
Defined (Level 2)

Comments: The CSB has defined policies, procedures, and processes in place to maintain an inventory of its information systems (including cloud- and third-party systems) and system interconnections. However, the Agency has not demonstrated that the inventory is comprehensive and accurate. Additionally, the CSB does not have a process or schedule for regularly reviewing and validating the inventory for accuracy, completeness, and alignment with operational and security requirements.

8. **FY25 Core:** To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including Government Furnished Equipment (GFE), Internet of Things [IoT], and Bring Your Own Device [BYOD] mobile devices) connected to the organization`s network with the detailed information necessary for tracking and reporting?
[RAM.02]
Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) and uses this taxonomy to inform which assets can or cannot be introduced into the network. The CSB was not assessed beyond a Level 3 because the Agency does not generate regular reports or metrics to assess the completeness and accuracy of the hardware asset inventory; nor does it track trends over time (for example, new assets detected, unapproved devices, asset retirement).

9. **FY25 Core:** To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting? [RAM.03]
Defined (Level 2)

Comments: The CSB has defined standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, considering Executive Order 14028 which includes critical software and mobile applications, used in the organization's environment. However, it does not use this taxonomy to determine which assets are introduced into the network. The CSB's inventory does not account for all installed software across the environment, particularly unauthorized or unmanaged software.

10. **FY25 Supplemental:** To what extent does the organization develop and maintain inventories of data and corresponding metadata for designated data types, as appropriate throughout the data lifecycle? [RAM.04]
Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented policies, procedures, processes, and roles and responsibilities to maintain a comprehensive and accurate inventory of its data and corresponding metadata, as appropriate. The CSB was not assessed beyond a Level 3 because the Agency has not established performance indicators to assess the completeness, accuracy, or timeliness of the data and metadata inventories, preventing the Agency from determining whether its inventory efforts are effective or improving.

11. **FY25 Core:** To what extent does the organization ensure that information system security risks are adequately managed? [RAM.05]

Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented its policies, procedures, and processes to manage the cybersecurity risks associated with operating and maintaining its information systems. The organization ensures that decisions to manage cybersecurity risk at the information system level are informed and guided by risk decisions made at the organizational and mission/business levels. While the CSB has risk management practices at various levels, the Agency was not assessed beyond a Level 3 because it does not use defined, quantifiable metrics to evaluate the effectiveness of those practices across the enterprise.

12. **FY25 Core:** To what extent does the organization use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?
[RAM.06]
Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented an automated solution across the enterprise that provides a centralized, enterprisewide view of cybersecurity risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. The CSB was not assessed beyond a Level 3 because the Agency does not use an integrated risk management tool to consolidate cybersecurity risks, control activities, and remediation efforts.

13.1 Please provide the assessed maturity level for the agency's Identify program.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within Risk and Asset Management, the domain is assessed as Level 2. We did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level. The maturity level for the Identify function is based on a calculated average of the individual metrics. We determined that the overall maturity for the Identify function is at Level 2.

13.2 Provide any additional information on the effectiveness (positive or negative) of the organizations RAM program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the RAM program effective?
[RAM.SUM]
We assessed the effectiveness of the CSB's information security program at Defined (Level 2). For metrics assessed at Level 3 or below, we documented justifications for those ratings.

Function 3A: Protect – Configuration Management

14. **FY25 Core:** To what extent does the organization use configuration settings/common secure configurations for its information systems?
[CM.01]
Defined (Level 2)

Comments: The CSB has defined procedures and processes in place to implement, assess, and maintain secure configuration settings for its information systems based on the principle of least functionality. The CSB also uses Security Content Automation Protocol-validated software assessing (scanning) capabilities against all systems on the network (in accordance with U.S. Department of Homeland Security Binding Operational Directive 23-01) to assess and manage both code-based and configuration-based vulnerabilities. However, the CSB did not provide details of the secure configuration settings. While the CSB has secure configuration standards defined, they may not be consistently implemented across all systems, platforms, or environments, leading to potential configuration drift and security gaps.

15. **FY25 Core:** To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP-assets?
[CM.02]
Consistently Implemented (Level 3)

Comment: The CSB has consistently implemented its flaw remediation policies, procedures, and processes and ensures that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner. In addition, the organization patches critical vulnerabilities within 30 days and uses lessons learned in implementation to make improvements to its flaw remediation policies and procedures. The CSB was not assessed beyond a Level 3 because the Agency lacks an enterprise wide, real-time dashboard that integrates asset discovery, vulnerability data, and remediation status, limiting visibility into the overall risk posture across business units.

16.1 Please provide the assessed maturity level for the agency's Protect - Configuration Management program.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within Configuration Management, the domain is assessed as Level 2. We did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

16.2 Provide any additional information on the effectiveness (positive or negative) of the organizations configuration management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?
[CM-SUM]
We assessed the effectiveness of the CSB's information security program at Defined (Level 2). For metrics assessed at Level 3 or below, we documented justifications for those ratings.

Function 3B: Protect – Identity and Access Management (IDAM)

17. **FY25 Core:** To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for non-privileged users to access the organization`s physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access?
[IDAM-01]
Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented strong authentication mechanisms for nonprivileged users of the organization's physical and logical assets (organization-defined entry/exit points) and networks, including for remote access and phishing-resistant Multifactor Authentication consistently for nonprivileged users. The CSB was not assessed beyond a Level 3 because the Agency does not track metrics such as Multifactor Authentication enrollment rates, phishing resistant Multifactor Authentication adoption by user group, or authentication failure rates. Without such data, there is no measurable basis for assessing implementation maturity.

18. **FY25 Core:** To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for privileged users to access the organization`s physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access?
[IDAM-02]
Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented strong authentication mechanisms for privileged users of the organization's physical and logical assets (organization-defined entry/exit points) and networks, including for remote access and phishing-resistant Multifactor Authentication consistently for privileged users. The CSB was not assessed beyond a Level 3 because the Agency does not track metrics such as Multifactor Authentication enrollment rates, phishing resistant Multifactor Authentication adoption by user group, or authentication failure rates. Without such data, there is no measurable basis for assessing implementation maturity.

19. **FY25 Core:** To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed? [IDAM-03]
Defined (Level 2)

Comments: The CSB has defined its policies and procedures to ensure that provisioning, managing, and reviewing privileged accounts is performed across the organization. However, it did not provide evidence that sufficient logs are maintained for monitoring and tracking user access and the historical usage of privileged accounts. The CSB does not consistently provision privileged access rights based on clearly defined job roles or functional requirements. Some users may not have elevated privileges that are necessary for their duties.

20.1 Please provide the assessed maturity level for the agency's Protect – Identity and Access Management (IDAM) program.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within Identity and Access Management, the domain is assessed as Level 2. We did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

20.2 Provide any additional information on the effectiveness (positive or negative) of the organizations IDAM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the IDAM program effective?
[IDAM-SUM]
We assessed the effectiveness of the CSB's information security program at Defined (Level 2). For metrics assessed at Level 3 or below, we documented justifications for those ratings.

Function 3C: Protect – Data Protection and Privacy

21. **FY25 Core:** To what extent has the organization implemented the following security controls to protect the confidentiality, integrity, and availability of its PII and other agency sensitive data, as appropriate, throughout the data lifecycle?

- Encryption of data at rest
- Encryption of data in transit
- Limitation of transfer to removable media
- Sanitization of digital media prior to disposal or reuse
- Backups of data are created, protected, maintained, and tested
- Access to personal email, external file sharing and storage sites, and personal communication applications are blocked, as appropriate.

[DPP.01]

Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented encryption for the specified areas, including (i) use of Federal Information Processing Standards-validated encryption of Personally Identifiable Information and other Agency-sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, (iii) destruction or reuse of media containing Personally Identifiable Information or other sensitive Agency data, (iv) backups of Personally Identifiable Information, including protection and testing of backups, and (v) access to personal email, external file-sharing and storage sites, and the blocking of personal communication applications, as appropriate. The CSB was not assessed beyond a Level 3 because the Agency has not established quantifiable metrics or dashboards to continuously measure and report on the implementation, performance, and effectiveness of data protection controls across systems and business units.

22. **FY25 Core:** To what extent has the organization implemented security controls (e.g., DLP, IDPS, CASB, User and Entity Behavior Analytic tools, SIEM and EDR) to prevent data exfiltration and enhance network defenses?
[DPP.02]
Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented the monitoring of inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing and malware and blocks against known malicious sites. Additionally, the organization checks outbound traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of Personally Identifiable Information. Also, suspected malicious traffic is quarantined or blocked. The CSB was not assessed beyond a Level 3 because the Agency does not routinely conduct penetration testing, red team exercises, or simulated exfiltration scenarios to validate whether the controls in place would effectively detect or block malicious activity.

23.1 Please provide the assessed maturity level for the agency's Protect – Data Protection and Privacy program.
Consistently Implemented (Level 3)

Comments: Based on the maturity level of the individual areas within Data Protection and Privacy, the domain is assessed as Level 3. We did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

23.2 Provide any additional information (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?
[DPP.SUM]
We assessed the effectiveness of the CSB's information security program at Consistently Implemented (Level 3). For metrics assessed at Level 3 or below, we documented justifications for those ratings.

Function 3D: Protect – Security Training

24. **FY25 Core:** To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide specialized security training within the functional areas of: govern, identify, protect, detect, respond, and recover? [ST.01]
Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented the assessment of the knowledge, skills, and abilities of its workforce; tailored its specialized training; and identified its skill gaps. Further, the organization periodically updates its assessment to account for a changing risk environment. In addition, the assessment serves as a key input to updating the organization's awareness and training strategy/plans. The CSB was not assessed beyond a Level 3 because the Agency does not consistently provide advanced or targeted training based on the specific security responsibilities for personnel in roles such as system administrators, incident responders, or developers.

25.1 Please provide the assessed maturity level for the agency's Protect – Security Training function.
Consistently Implemented (Level 3)

Comments: Based on the maturity level of the individual areas within Security Training, the domain is assessed as Level 3. We did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

25.2 Please provide the assessed maturity level for the agency's Protect program.
Defined (Level 2)

Comments: The maturity level for the Protect function is based on a calculated average of the individual metrics. We determined that the overall maturity for the Protect function is at Level 2.

25.3 Provide any additional information (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the security training program effective?
[ST.SUM]
We assessed the effectiveness of the CSB's information security program at Consistently Implemented (Level 3). For metrics assessed at Level 3 or below, we documented justifications for those ratings.

Function 4: Detect – Information Security Continuous Monitoring (ISCM)

26. **FY25 Core:** To what extent does the organization use information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier?
[ISCM.01]
Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented the Information Security Continuous Monitoring policies and strategy at the organization, business process, and information system levels. In addition, the strategy supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captures lessons learned to make improvements to the Information Security Continuous Monitoring policies and strategy. The CSB was not assessed beyond a Level 3 because the Agency does not use clearly defined metrics to measure the effectiveness, frequency, and coverage of Information Security Continuous Monitoring activities. Without these measurable outcomes, there is no basis for assessing program maturity or improving control effectiveness.

27. **FY25 Supplemental:** To what extent does the organization monitor and measure the integrity and security posture of all owned and associated assets?
[ISCM.02]
Defined (Level 2)

Comments: The CSB has defined procedures in place to analyze the data it collects on potentially adverse events to better understand associated activities, as well as monitoring and enforcement mechanisms to identify and manually disconnect or isolate noncompliant devices and virtual assets. Additionally, the Agency employs network monitoring capabilities based on known indicators of compromise to develop situational awareness and correlates telemetry from multiple sources for analysis and monitoring. However, the Agency has not provided evidence that all devices attached to the network are appropriately identified. The CSB's asset inventory is not actively monitored to ensure that all assets are identified and appropriately categorized, potentially reducing completeness and accuracy of these records.

28. **FY25 Core:** To what extent does the organization performing ongoing (continuous monitoring) information system assessments to grant system authorizations, including developing and maintaining system security plans, and monitoring system security controls?
[ISCM.03]
Consistently Implemented (Level 3)

Comments: The CSB consistently implemented its system level continuous monitoring strategies and related processes, including performing ongoing security control assessments, granting system authorizations, and monitoring security controls to provide a view of the organizational security posture, as well as each system's contribution to said security posture. The CSB was not assessed beyond a Level 3 because the Agency does not have an enterprisewide view of system authorization status, overdue plans of action and milestones, or incomplete assessments. Without this centralized reporting mechanism, it may be difficult to identify trends or manage risk across the portfolio of systems.

29.1 Please provide the assessed maturity level for the agency's Detect function.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within Information Security Continuous Monitoring, the domain is assessed as Level 2. We did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level. The maturity level for the Detect function is based on a calculated average of the individual metrics. We determined that the overall maturity for the Detect function is at Level 2.

29.2 Provide any additional information on the effectiveness (positive or negative) of the organizations ISCM program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?
[ISCM.SUM]
We assessed the effectiveness of the CSB's information security program at Defined (Level 2). For metrics assessed at Level 3 or below, we documented justifications for those ratings.

Function 5: Respond – Incident Response

30. **FY25 Core:** To what extent has the organization implemented processes related to incident detection and analysis? [IR.01]
Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented enterprisewide policies, procedures, and processes for incident detection and analysis. In addition, the organization consistently uses its enterprisewide threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. The CSB was not assessed beyond a Level 3 because the Agency does not use performance metrics to assess and improve the performance of its incident detection and analysis processes.

31. **FY25 Core:** To what extent has the organization implemented processes related to incident handling? [IR.02]
Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented enterprisewide incident handling policies and procedures, containment strategies, and incident eradication processes. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident handling policies and procedures and making updates as necessary. The CSB was not assessed beyond a Level 3 because the Agency does not define or track metrics such as incident recurrence rates or containment success rates. Without measurable indicators, the effectiveness of incident handling processes cannot be evaluated or improved.

32.1 Please provide the assessed maturity level for the agency's Respond program.
Consistently Implemented (Level 3)

Comments: Based on the maturity level of the individual areas within Incident Response, the domain is assessed as Level 3. We did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level. The maturity level for the Respond function is based on a calculated average of the individual metrics. We determined that the overall maturity for the Respond function is at Level 3.

32.2 Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the incidence response effective?
[IR.SUM]
We assessed the effectiveness of the CSB's information security program at Consistently Implemented (Level 3). For metrics assessed at Level 3 or below, we documented justifications for those ratings.

Function 6: Recover – Contingency Planning

33. **FY25 Core:** To what extent does the organization ensure that the results of BIAs are used to guide contingency planning efforts? [CP.01]

Defined (Level 2)

Comments: The CSB has defined its policies, procedures, and processes for conducting organizational and system-level business impact analyses and for incorporating the results into strategy and plan development efforts, such as its incident response plan, information system contingency plans, and continuity of operations plan. The CSB does not perform BIAs on a defined schedule, making it unlikely that contingency plans reflect the current business impact and operational priorities.

34. **FY25 Core:** To what extent does the organization perform tests/exercises of its information system contingency planning processes? [CP.02]

Defined (Level 2)

Comments: The CSB has defined policies, procedures, and processes for information system contingency plan testing and exercises that include, as applicable, notification procedures, system recovery on an alternate platform from backup media, internal and external connectivity, system performance using alternate equipment, restoration of normal procedures, coordination with other business areas/continuity plans, and tabletop and functional exercises. The CSB does not conduct contingency plan tests or exercises on a regular, predefined schedule. Tests may be performed reactively rather than proactively to validate readiness.

35.1 Please provide the assessed maturity level for the agency's Recover Program.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within Contingency Planning, the domain is assessed as Level 2. We did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level. The maturity level for the Recover function is based on a calculated average of the individual metrics. We determined that the overall maturity for the Recover function is at Level 2.

35.2 Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the contingency planning program effective?
[CP.SUM]
We assessed the effectiveness of the CSB's information security program at Defined (Level 2). For metrics assessed at Level 3 or below, we documented justifications for those ratings.

APPENDIX A: Maturity Model Scoring

A.1 Please provide the assessed maturity level for the agency's Overall status.

Function	FY25 Core	FY25 Supplemental	FY25 Weighted Average	FY25 Assessed Maturity	FY25 Effectiveness	Explanation
Govern	2.00	2.67	2.57	Defined (Level 2)	Not Effective	The maturity level for the Govern function is based on a calculated average of the individual metrics. We determined that the overall maturity for the Govern function is at Level 2.
Identify	2.60	3.00	2.60	Defined (Level 2)	Not Effective	The maturity level for the Identify function is based on a calculated average of the individual metrics. We determined that the overall maturity for the Identify function is at Level 2.
Protect	2.75	—	2.75	Defined (Level 2)	Not Effective	The maturity level for the Protect function is based on a calculated average of the individual metrics. We determined that the overall maturity for the Protect function is at Level 2.
Detect	3.00	2.00	3.00	Defined (Level 2)	Not Effective	The maturity level for the Detect function is based on a calculated average of the individual metrics. We determined that the overall maturity for the Detect function is at Level 2.
Respond	3.00	—	3.00	Consistently Implemented (Level 3)	Not Effective	The maturity level for the Respond function is based on a calculated average of the individual metrics. We determined that the overall maturity for the Respond function is at Level 3.
Recover	2.00	—	2.00	Defined (Level 2)	Not Effective	The maturity level for the Recover function is based on a calculated average of the individual metrics. We determined that the overall maturity for the Recover function is at Level 2.

Function	FY25 Core	FY25 Supplemental	FY25 Weighted Average	FY25 Assessed Maturity	FY25 Effectiveness	Explanation
Overall Maturity	**2.56**	**2.56**	**2.65**	Defined (Level 2)	Not Effective	The U.S. Chemical Safety and Hazard Investigation Board's Information Technology Security Program has demonstrated that it has defined policies, procedures and strategies for the Govern, Identify, Protect, Detect, and Recover information security function areas and consistently implemented for the Respond Function Area. The U.S. Environmental Protection Agency Office of Inspector General contracted SB & Company LLC to assess the six Cybersecurity Framework function areas, and the contractor concluded that the CSB has achieved a Level 2 (Defined) maturity, which denotes that the CSB has defined policies, procedures, and strategies in adherence to the FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0. The CSB's Information Technology Security Program is therefore considered not effective.

Appendix B

Status of CSB Corrective Actions for FY 2024 FISMA Audit Recommendations

The table below details the OIG's analysis of the corrective actions that the CSB has implemented for the recommendations issued in OIG Report No. 25-P-0037, *Audit of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024*, dated June 17, 2025.

Recommendation		Corrective Action	OIG analysis of corrective action status
1	Develop a process for designating and maintaining personnel in key roles (permanent and/or temporary) to ensure the continuity of essential security functions including the availability to respond to FISMA inquiries.	**Implemented** The CSB hired a deputy chief information officer in September 2024. The deputy chief information officer resigned from the Agency and an acting deputy chief information officer was appointed in March 2025.	**Closed**-Corrective Action Completed

Appendix C

CSB Response to Draft Report

U.S. Chemical Safety and Hazard Investigation Board

470 L'Enfant Plaza SW, Suite 604 #23278 | Washington, DC 20026
Phone: (202) 261-7600 | www.csb.gov

Steve Owens
Chairperson

Sylvia E. Johnson, Ph.D.
Board Member

April 30, 2026

Ms. Michelle Wicker
Director, Information Resource Management
U.S. EPA Office of Inspector General
109 T.W. Alexander Drive
Durham, NC 27711

Dear Ms. Wicker:

The U.S. Chemical Safety and Hazard Investigation Board (CSB) appreciates the opportunity to comment on the EPA Office of Inspector General's (OIG) draft report entitled, *U.S. Chemical Safety and Hazard Investigation Board's Federal Information Security Modernization Act of 2014 Audit Report for Fiscal Year 2025* (Project No. OA-FY25-0042).

The CSB concurs with the findings and recommendations in the draft report. The CSB has continued to make significant improvements to the agency's information security posture in fiscal year 2025. As the draft report notes, the CSB's Information Technology Security Program has demonstrated that it has defined policies, procedures, and strategies for the Govern, Identify, Protect, Detect, and Recover information security function areas and consistently implemented these for the Respond function area.

The CSB provides the following regarding the four recommendations in the draft report:

Recommendation 1: The CSB already has implemented an asset management system that is audited and updated on a rolling 12-month cycle. Recommendation 1 has been completed on September 20, 2025.

Recommendation 2: On September 12, 2025, the CSB generated an alert and log of notifications of the Privileged Identity Management account activations and de-activations for any administrative roles. This control, the secure mailbox process, is being implemented following the 2025 audit findings, with all records maintained for a three-year retention period. Estimated completion date for recommendation 2 is September 15, 2026.

Recommendation 3: The secure mailbox represents an interim method for monitoring and storing user authentication logs, and the CSB is currently working with Microsoft to implement, by September 30, 2026, an automated storage environment and pipeline for maintaining these logs. These logs include user logins and privileged escalations that will be maintained for a three-year retention period. Estimated completion date for recommendation 3 is September 15, 2026.

Recommendation 4: Contingency planning activities and FY 2026 tabletop exercises will be conducted with both leadership and all staff to ensure awareness and testing of continuity procedures during April 2026. As part of the agency's transition to a cloud-based environment, the CSB has implemented Azure-based backups that are automatically validated through built-in integrity checks. The CSB also will conduct an annual test to confirm Recovery Time Objective (RTO) and Recovery Point Objective (RPO) performance for the agency's servers. The results of this test will be documented as part of the CSB's continuity program. Estimated completion date for recommendation 4 is April 20, 2026.

Regards,

Sabrina Morris
Director of Administration

Appendix D

Distribution

Chairperson
General Counsel
Board Members
EPA OIG Liaison
Director of Administration/Board Affairs
Information Technology Director/Chief Information Officer
Financial Management Specialist
Director of Financial Operations

Whistleblower Protection

U.S. Environmental Protection Agency

The whistleblower protection coordinator's role is to educate agency employees about prohibitions against retaliation for protected disclosures and the rights and remedies against retaliation. For more information, please visit our website.

Contact us:

Congressional & Media Inquiries: OIG.PublicAffairs@epa.gov

EPA OIG Hotline: OIG.Hotline@epa.gov

Web: epa.gov/oig

Follow us:

X: @epaoig

LinkedIn: linkedin.com/company/epa-oig

YouTube: youtube.com/epaoig

Instagram: @EPA_OIG

www.epa.gov/oig