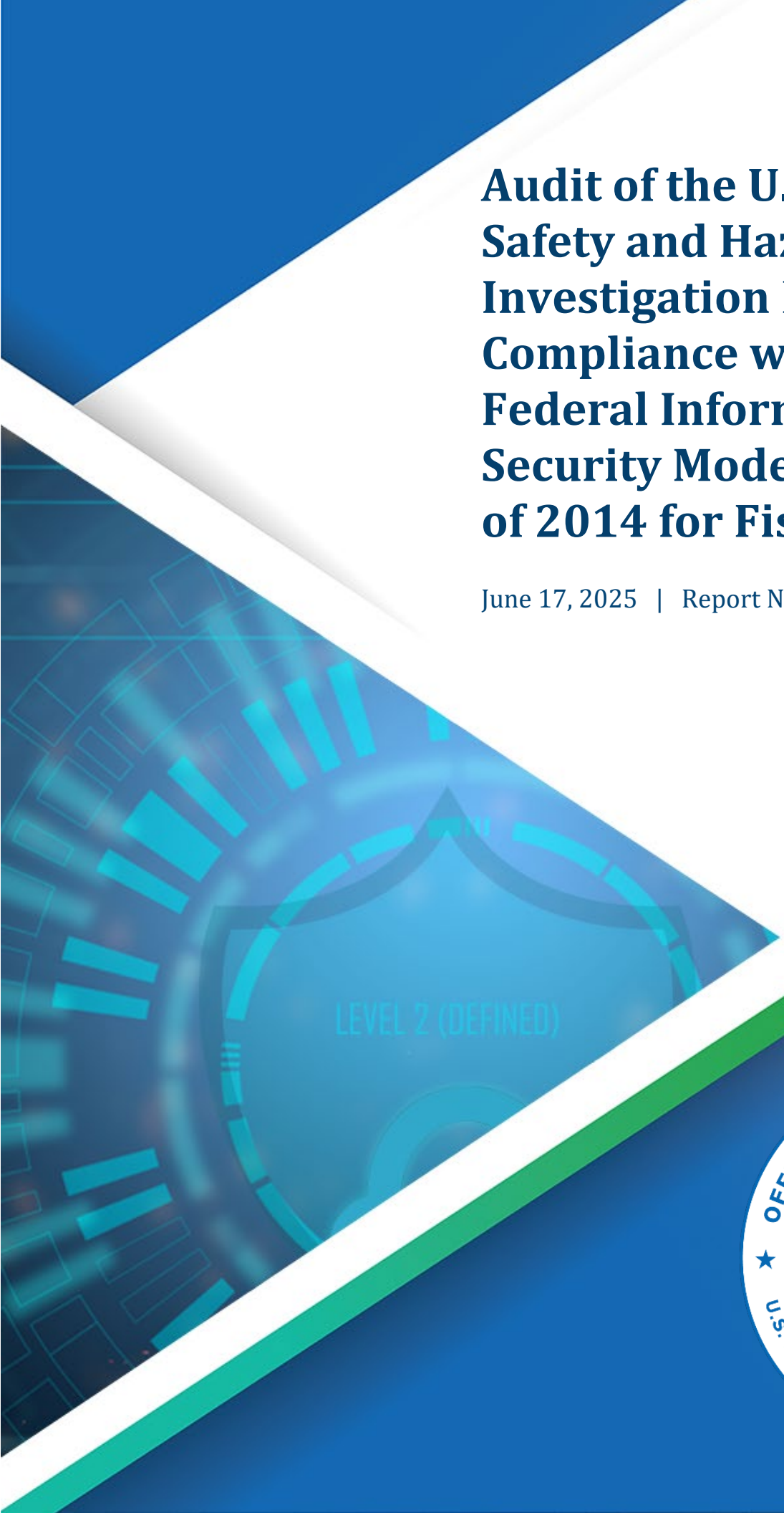
Audit of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024

June 17, 2025 | Report No. 25-P-0037



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

A technology-themed image with the text “Level 2 (Defined),” representing that the CSB’s information security program for fiscal year 2024 was rated at Level 2. (EPA OIG image)

25-P-0037
June 17, 2025

At a Glance

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

Why This Audit Was Performed

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 *Fiscal Year 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* during fiscal year 2024. We contracted with SB & Company LLC to perform this audit under our direction and oversight.

The *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 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 concluded that the CSB achieved an overall maturity of Level 2, Defined, in fiscal year 2024. 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 Defined maturity level that it achieved in fiscal year 2023, SB & Company identified an area of needed improvement associated with the *Reporting Metrics'* Risk Management domain in the Identify function area. SB & Company concluded that the CSB should ensure that its information can be reliably accessed in a timely manner even if key personnel are absent. Specifically, the CSB should ensure that its deputy chief information officer position is filled or that another CSB representative is available to respond to Federal Information Security Modernization Act of 2014 inquiries. CSB Board Order 034, *Information Technology Security Program,* states that the chief information officer is responsible for ensuring that appropriate resources are allocated to the CSB's Information Technology Security Program and for selecting an individual to serve as the deputy chief information officer. If the CSB does not ensure that key roles and responsibilities are backed up, it risks the timely execution of tasks and hinders the access and availability of information.

> **The deputy chief information officer plays a key role in maintaining the continuity of CSB operations and preserving institutional knowledge if the chief information officer is unavailable.**

Recommendation and Planned Agency Corrective Action

SB & Company made one recommendation to the CSB, and we agree with and adopt the recommendation. SB & Company recommended that the CSB "[d]evelop a process for designating and maintaining personnel in key roles (permanent and/or temporary) to ensure the continuity of essential security functions," including availability to respond to Federal Information Security Modernization Act of 2014 inquiries. As of March 2025, an information technology specialist is serving as acting deputy chief information officer and can serve as a backup for the chief information officer according to CSB Board Order 034. Therefore, we consider the corrective action for this recommendation to be completed.

The CSB believes that it has met the threshold for maturity Level 3, despite its overall maturity being assessed at Level 2. However, the reporting metrics focused on a calculated average approach, wherein the average of the metrics in a particular domain was used to determine the effectiveness of the overall program. Because the majority of metrics were rated at Level 2, the CSB's overall calculated maturity level resulted in a Level 2 rating.

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

June 17, 2025

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 information technology security work performed by SB & Company LLC, under the direction of the U.S. Environmental Protection Agency Office of Inspector General. This report also includes SB & Company's completed fiscal year 2024 Federal Information Security Management Act of 2014 reporting template, as prescribed by the Office of Management and Budget. The project number for this audit was OA-FY24-0097.

The report contains SB & Company's finding and recommendation. We agree with SB & Company's recommendation and adopt it as our own.

Your office provided a response to SB & Company's recommendation. SB & Company will conduct follow-up in FY 2025 to determine the status of the recommendation. You are not required to respond to this report. If you submit a response, however, it will be posted on the OIG's website, along with our memorandum commenting on your response. Your 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 you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal along with corresponding justification.

We will post this report to our website at www.epaoig.gov.

Sincerely,

Nicole N. Murley

Nicole N. Murley
Acting Inspector General

Table of Contents

Appendixes

Certified Public Accountants & Business Advisors
SBC

Report of Independent Public Accountants

Management
U.S. Chemical Safety and Hazard Investigation Board
Washington, DC

SB and Company LLC conducted a performance audit of the U.S. Chemical Safety and Hazard Investigation Board's (CSB) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). 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 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 September of 2020.

For this audit, we reviewed CSB's information technology systems. Audit fieldwork covered the CSB's headquarters located in Washington, DC, from October 1, 2023, to June 15, 2024. 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We determined that CSB's overall information security program "Defined" because the majority of the FY 2024 FISMA core IG and FY 2024 supplemental metrics were rated Defined (Level 2). In our report, we have provided the Chief Information Officer (CIO) one finding and one recommendation that when addressed should strengthen CSB's information security program. The CSB CIO disagreed with our conclusion and recommendation (see Management Response, page 11).

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

Washington, D.C.
March 11, 2025

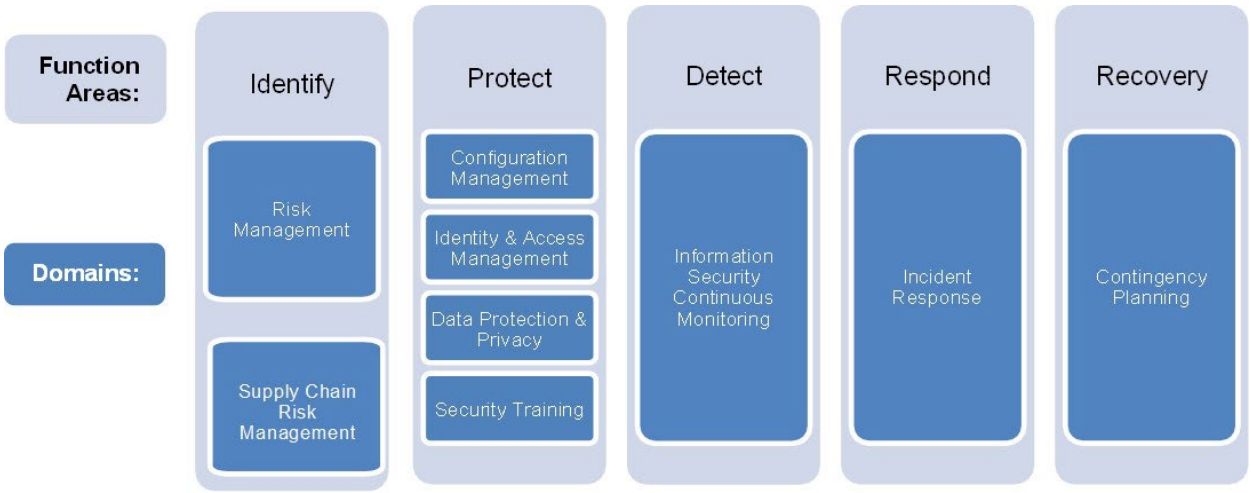
SB & Company, LLC

Background

Under the Federal Information Security Modernization Act of 2014 (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 U.S. Department of Homeland Security and the Office of Management and Budget issue 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 *Fiscal Year (FY) 2023 - 2024 FISMA Reporting Metrics* [1] which can be found in Appendix A, provides 20 core metrics and 20 metrics to be reviewed in FY24 across the five function areas' nine domains to be assessed to provide sufficient data to determine the effectiveness of an Agency's information security program with a high level of confidence (Figure 1).[2] This cybersecurity framework provides agencies with a common structure for identifying and managing cybersecurity risks to critical infrastructure across the enterprise.

Figure 1: FY 2024 cybersecurity framework security function areas and domains



Source: OIG-created graphic based on *FY 2024 IG FISMA Reporting Metrics* information. (EPA OIG image)

[1] *Fiscal Year (FY) 2023 - 2024 FISMA Reporting Metrics*. These metrics were developed as a collaborative effort between the Office of Management and Budget, the Department of Homeland Security, and the Council of the Inspectors General on Integrity Management and Efficiency, in consultation with the Federal Chief Information Officer Council.

[2] Executive Order 13636, Improving Critical Infrastructure Cybersecurity, was issued February 19, 2013, and directed NIST to develop a voluntary 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 (Table 1). An agency's IG 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 nine domains. The IG 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.

Table 1: Maturity model spectrum

Maturity level		Description
1	Ad Hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad hoc, reactive manner.
2	Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
3	Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
4	Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures and strategies are collected across the organization and used to assess them and make necessary changes.
5	Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: *FY 2024 IG FISMA Reporting Metrics*.

Scope and Methodology

SB & Company, LLC (SBC or We) conducted this audit from May to July 2024 in accordance with Government Auditing Standards (Yellow Book) standards.

During our audit, we assessed whether the CSB exceeded Maturity Level 2, *Defined*, for each of the 66 questions for the nine domains in the *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* and the *FY 2024 Core IG Metrics Implementation Analysis and Guidelines*. We conducted a risk assessment of the FY 2024 IG FISMA metrics to determine whether changes made to the underlying criteria of the FISMA metric questions significantly changed since the FY 2023 audit.

We also evaluated the new FY 2024 criteria to assess whether they significantly changed the CSB's responses to the overall metric questions since the FY 2023 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 2023 audit for the identified metric question.

- Low Risk—The CSB made no significant changes to its information security program since the FY 2023 audit for the identified metric question.

We relied on the responses to the FY 2023 CSB FISMA metric questions to answer the FY 2024 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 the CSB and briefed the agency on the audit results for each function area of the *Fiscal Year (FY) 2023 - 2024 FISMA Reporting Metrics.*

Appendix A provides the OIG response to each FISMA metric, as submitted to the Office of Management and Budget by July 31, 2024.

Prior Audit

During our testing of the CSB's FY 2024 FISMA compliance, SBC followed up on deficiencies identified in the FY 2023 FISMA audit, as documented in Report No. **24-P-0035** The CSB Has Improved Its Information Security Program but Needs to Document Recovery Testing Results, Consistent with National Institute of Standards and Technology Guidelines, dated April 29, 2024. We reported that the CSB did not formally document lessons learned during Disaster Recovery testing and needed improvement in one domain: (8) "Incident Response". Specifically, SBC found that the CSB did not:

1) Record the Disaster Recovery testing scenarios and the lessons learned during the test.

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

Results

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

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

Function area	Domain	Overall OIG-assessed maturity level
Identify	Risk Management	Level 2, *Defined*
Identify	Supply Chain Risk 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 2, *Defined*
Recover	Contingency Planning	Level 2, *Defined*

Source: *FY 2024 IG FISMA Reporting Metrics*.

However, in FY 2024, the CSB continued to need improvements for a specific question in the "Risk Management" domain, as shown in Table 3.

Table 3: CSB domains that require further improvement

Function area	Domain	FISMA questions that need improvement
Identify	Risk Management	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 availability and continuity of personnel resources. During the course of the audit, the CSB's Deputy CIO position remained vacant. CSB designated staff as a Deputy CIO but they were not authorized to provide FISMA related documentation in the CIO's absence. The CSB should ensure timely and reliable access to information in the absence of key personnel, by ensuring that the Deputy CIO position is filled or another representative from the CSB is available to respond to FISMA inquiries.

Source: SBC Recap

The overall assessed level of the information security program was determined to be *Level 2-Defined* as all questions were considered equally during the assessment. The CSB continues to make significant progress in updating the CSB's cyber security

program and ensuring that it upgrades security policies, tools, and practices as they evolve.

Conclusion

The CSB would improve and strengthen its cybersecurity program by developing a process for designating and maintaining personnel in key roles (permanent and/or temporary) to ensure the continuity of essential security functions. This would provide continuity in the organization, as well as decreasing their risk exposure, increasing their compliance and accountability, providing for knowledge transfer, and training, and ensuring their preparedness for emergencies. This process should include ensuring that the Deputy CIO position is filled or another representative from the CSB is available to respond to FISMA inquiries.

Recommendations

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

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.

CSB Response and Procedures Performed

The CSB disagrees with the notice of recommendation as we have ensured that the Office of the CIO is fully staffed with a Chief Information Officer (CIO), Deputy Chief Information Officer (DCIO), an IT Specialist, and a Records and Information Management Specialist. In the event that the CIO is not available, the DCIO and IT Specialist are able to provide coverage for the CIO.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Potential Monetary Benefits (in $000s)
1	6	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.	C	Chairperson		

[1] 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 Department of Homeland Security's CyberScope program by the EPA OIG, based on the template completed by SB & Company.

Inspector General

Section Report

2024

Chemical Safety Board

Function 0: Overall

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

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 all five information security function areas. The U.S. Environmental Protection Agency Office of Inspector General contracted SB and Company LLC to assess the five 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 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics." 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 availability and continuity of personnel resources. The CSB should ensure timely and reliable access to information in the absence of key personnel.

Function 1A: Identify – Risk Management

1. **FY24 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?
Consistently Implemented (Level 3)

Comments : The CSB has consistently implemented processes and procedures to maintain a comprehensive inventory of its information systems. The information systems inventory is maintained and is current.

2. **FY24 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 GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?
Defined (Level 2)

   Comments : The CSB has defined a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory. The hardware inventory is maintained and current.

3. **FY24 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?
Defined (Level 2)

   Comments : The CSB has defined a process for using standard data elements or taxonomy to develop and maintain an up-to-date inventory of the software licenses used in the organization's environment, with the detailed information necessary for tracking and reporting. The inventory is maintained and is current.

4. **FY24 Supplemental:** To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets?
Defined (Level 2)

   Comments : The CSB's "Information Security Continuous Monitoring Plan" has categorized and communicated the importance and priority of information systems in enabling its missions and business functions, including for high-value assets.

5. **FY24 Core:** To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels?
Defined (Level 2)

Comments : The CSB has defined and communicated the policies, procedures, and processes that it uses to manage the cybersecurity risks associated with operating and maintaining its information systems.

6. **FY24 Supplemental:** To what extent does the organization use an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain?
Defined (Level 2)

   Comments : The CSB has defined an information security architecture and described how that architecture is integrated into and supports the CSB's enterprise architecture.

7. **FY23 Supplemental:** To what extent have the roles and responsibilities of internal and external stakeholders involved in cybersecurity risk management processes been defined, communicated, implemented, and appropriately resourced across the organization?
Defined (Level 2)

8. **FY23 Supplemental:** To what extent has the organization ensured that plans of action and milestones (POA&Ms) are used for effectively mitigating security weaknesses?
Defined (Level 2)

9. **FY23 Supplemental:** To what extent does the organization ensure that information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders?
Defined (Level 2)

10. **FY24 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?
Defined (Level 2)

    Comments : The CSB has defined how cybersecurity risks are communicated in a timely and effective manner to appropriate internal and external stakeholders. Additionally, the CSB performs an annual risk assessment, measuring its security posture against National Institute of Standards and Technology 800-53, Revision 5, dated September 2020, (including updates as of December 2020)

11.1 Please provide the assessed maturity level for the agency's Identify - Risk Management program.
Defined (Level 2)

Comments : Based on the maturity level of the individual areas within Risk Management domain, the domain is assessed as "Defined."

11.2 Provide any additional information on the effectiveness (positive or negative) of the organizations 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 risk management program effective?
Based on the maturity level of the individual areas within the Risk Management Program, the domain is assessed as "Defined." We limited our testing to those questions that would materially change our fiscal year 2023 response. For those metrics with policies, procedures, and strategies, we rated the CSB at Level 2 (Defined). However, we did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

Function 1B: Identify – Supply Chain Risk Management

12. **FY23 Supplemental:** To what extent does the organization use an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?
Defined (Level 2)

13. **FY23 Supplemental:** To what extent does the organization use SCRM policies and procedures to manage SCRM activities at all organizational tiers?
Defined (Level 2)

14. **FY24 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?
Defined (Level 2)

Comments : The CSB has procedures in place to ensure that products, system components, systems, and services of external providers are consistent with their cybersecurity and supply chain requirements through the exclusive use of vendors approved by the U.S. General Services Administration.

15. **FY24 Supplemental:** To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization's systems?
Defined (Level 2)

Comments : The CSB ensures that counterfeit components are prevented from entering the organization's systems through the exclusive use of vendors approved by the General Services Administration.

16.1 Please provide the assessed maturity level for the agency's Identify - Supply Chain Risk Management program.
Defined (Level 2)

Comments : Based on the maturity level of the individual areas within the Supply Chain Risk Management program, the domain is assessed as "Defined."

16.2 Please provide the assessed maturity level for the agency's Identify Function.
Defined (Level 2)
Comments : Based on the maturity level of the individual areas within the Risk Management and Supply Chain Risk Management domains, the Identify function is assessed as "Defined." We limited our testing to those questions that would materially change our fiscal year 2023 response.

16.3 Provide any additional information on the effectiveness (positive or negative) of the organizations 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 risk management program effective?
Based on the maturity level of the individual areas within Supply Chain Risk Management Program, the domain is assessed as "Defined." We limited our testing to those questions that would materially change our fiscal year 2023 response. For those metrics with policies, procedures, and strategies, we rated the CSB at Level 2 (Defined). However, we did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

Function 2A: Protect – Configuration Management

17. **FY24 Supplemental:** To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?
Defined (Level 2)

Comments : The CSB's "Configuration Management Policy" defines roles and responsibilities and communicates them across the organization at both the organizational and information system levels for stakeholders involved in information system configuration management.

18. **FY24 Supplemental:** To what extent does the organization use an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems?
Defined (Level 2)

Comments : The CSB's "Configuration Management Policy" defines roles and responsibilities for configuration management, including processes for change management and the System Development Life Cycle.

19. **FY23 Supplemental:** To what extent does the organization use baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting?
Defined (Level 2)

20. **FY24 Core:**To what extent does the organization use configuration settings/common secure configurations for its information systems?
Defined (Level 2)

Comments : The CSB has defined its policies and procedures for configuration settings and or common secure configurations. In addition, the CSB has defined common secure configurations, or hardening guides, that are tailored to its environment.

21. **FY24 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?
Defined (Level 2)

Comments: The CSB has an information technology Plan of Action and Milestones tracking sheet for vulnerability management, which includes a time frame for remediating vulnerabilities. The tracking sheet also includes documented procedures that define how the tracking sheet will be used to mitigate any identified security weaknesses.

22. **FY23 Supplemental:** To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network?
Defined (Level 2)

23. **FY24 Supplemental:** To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, asappropriate?
Defined (Level 2)

Comments: The CSB's "Configuration Management Policy" defines the policies and procedures for managing configuration change control that the CSB has developed, documented, and disseminated.

24. **FY23 Supplemental:** To what extent does the organization use a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet- accessible federal systems?
Defined (Level 2)

25.1 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 the Configuration Management program, the domain is assessed as "Defined."

25.2 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 maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?
Based on the maturity level of the individual areas within the Configuration Management Program, the domain is assessed as "Defined." We limited our testing to those questions with criteria added to the metric that would materially change our fiscal year 2023 response. However, we did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

Function 2B: Protect – Identity and Access Management

26. **FY23 Supplemental:** To what extent have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?
Defined (Level 2)

27. **FY23 Supplemental:** To what extent does the organization use a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities?
Consistently Implemented (Level 3)

28. **FY24 Supplemental:** To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems?
Defined (Level 2)

Comments: The CSB has defined its processes for ensuring that all personnel are assigned risk designations and appropriately screened prior to being granted access to its systems. The CSB also has defined processes for authorizing access following screening completion and periodic rescreening of individuals.

29. **FY23 Supplemental:** To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained?
Defined (Level 2)

30. **FY24 Core:** To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDOor web authentication) for non- privileged users to access the organization`s facilities [organization-defined entry/exit points], networks, and systems, including for remote access?
Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented strong authentication mechanisms in the use of a Virtual Private Network to remotely access the internal network. In addition to logical access to the systems, the CSB also has controls in place to limit physical access to its Local Area Network (server) room using electronic locks, limiting access to appropriate personnel, accompanying visitors, and recording visitor access.

31. **FY24 Core:** To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDOor web authentication) for privileged users to access the organization`s facilities [organization-defined entry/exit points], networks, and systems, including for remote access?
Consistently Implemented (Level 3)

Comments : The CSB has consistently implemented strong authentication mechanisms for privileged users of the organization’s facilities including multifactor authentication on the Virtual Private Network used to remotely access the internal network.

32. **FY24 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?
Defined (Level 2)

Comments: The CSB has defined its processes for provisioning, managing, and reviewing privileged accounts.

33. **FY23 Supplemental:** To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote accesssessions?
Defined (Level 2)

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

Comments: Based on the maturity level of the individual areas within the Identity and Access Management program, the domain is assessed as "Defined."

34.2 Provide any additional information on the effectiveness (positive or negative) of the organizations identity and access management 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 identity and access management program effective?
Based on the maturity level of the individual areas within Identity and Access Management Program, the domain is assessed as "Defined." We limited our testing to those questions with criteria added to the metric that would materially change our fiscal year 2023 response. For those metrics with documented policies, procedures, and strategies, we rated the CSB at Level 2 (Defined). However, we did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

Function 2C: Protect – Data Protection and Privacy

35. **FY23 Supplemental:** To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems?
Defined (Level 2)

36. **FY24 Core:** To what extent has the organization implemented the following security controls to protect 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.

    Defined (Level 2)

    Comments: The CSB has defined, as well as communicated, its policies and procedures for the encryption of data at rest and in transit, the limitation of transference of data by removable media, and the sanitization of digital media prior to disposal or reuse to protect its personally identifiable information and other sensitive data, as appropriate. Additionally, the policies and procedures have been tailored to the CSB's environment and include specific considerations based on data classification and sensitivity.

37. **FY24 Core:** To what extent has the organization implemented security controls (e.g., EDR) to prevent data exfiltration and enhance network defenses?
Defined (Level 2)

    Comments: The CSB defined the organization's implemented security controls to prevent data exfiltration and enhance network defenses.

38. **FY24 Supplemental:** To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?
Defined (Level 2)

    Comments: The CSB has defined and implemented its "Data Breach Response Plan," including processes and procedures for data breach notification. Additionally, a Breach Response Team has been established that includes the appropriate CSB officials.

39. **FY24 Supplemental:** To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role- based privacy training?(Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of and E- Government Act of 20consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and user requirements).
Defined (Level 2)

Comments: The CSB has defined its Privacy Awareness Training Program based on the organizational requirements, culture, and types of personally identifiable information or protected health information that its users have access to. Additionally, periodic privacy training is provided to users based on their roles.

40.1 Please provide the assessed maturity level for the agency's Protect - Data Protection and Privacy program.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within the Data Protection and Privacy program, the domain is assessed as "Defined."

40.2 Provide any additional information on the effectiveness (positive or negative) of the organizations data protection and privacy 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 data protection and privacy program effective?
Based on the maturity level of the individual areas within Data Protection and Privacy Program, the domain is assessed as "Defined." We limited our testing to those questions with criteria added to the metric that would materially change our fiscal year 2023 response. For those metrics with documented policies, procedures, and strategies, we rated the CSB at Level 2 (Defined). However, we did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

Function 2D: Protect – Security Training

41 **FY23 Supplemental:** To what extent have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?Note: This includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant securityresponsibilities.
Defined (Level 2)

42 **FY24 Core:** To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover?
Defined (Level 2)

Comments: The CSB's security training is provided annually, is used to access the skills of the CSB's workforce, and is tailored to cover specific awareness and specialized security topics.

43 **FY23 Supplemental:** To what extent does the organization use a security awareness and training strategy/plan that leverages its skills assessment and is adapted to its mission and risk environment? Note: The strategy/plan should include the following components:

- The structure of the awareness and training program
- Priorities
- Funding
- The goals of the program
- Target audiences
- Types of courses/ material for each audience
- Use of technologies (such as email advisories, intranet updates/wiki pages/social media, web- based training, phishing simulation tools)
- Frequency of training
- Deployment methods

Consistently Implemented (Level 3)

44 **FY24 Supplemental:** To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting?
Defined (Level 2)

Comments: Processes are in place for tracking the completion of security awareness training. These include employee attestation to the completion of the security awareness training and follow-up to identify individuals that have not completed training requirements.

45 **FY24 Supplemental:** To what extent does the organization ensure that specialized security training is provided to individuals with significant security responsibilities (as defined in the organization`s security policies and procedures and in accordance with 5 Code of Federal Regulation 930.301)?
Consistently Implemented (Level 3)

Comments: Processes are in place for ensuring that specialized security training for individuals with security responsibilities is provided. These include attendance at webinars and participation in conferences and other training events.

46.1 Please provide the assessed maturity level for the agency's Protect - Security Training program.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within the Security Training program, the domain is assessed as “Defined.”

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

Comments: Based on the maturity level of the individual areas within the Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains , the Protect function is assessed as “Defined.”

46.3 Provide any additional information on the effectiveness (positive or negative) of the organizations security training 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 security training program effective?
Based on the maturity level of the individual areas within the Security Training Program, the domain is assessed as "Defined." We limited our testing to those questions with criteria added to the metric that would materially change our fiscal year 2023 response. For those metrics with documented policies, procedures, and strategies, we rated the CSB at Level 2 (Defined). However, we did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

Function 3: Detect – ISCM

47 **FY24 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?
Defined (Level 2)

Comments: The CSB's "Information Security Continuous Monitoring Plan" [ISCM] and strategy is tailored to the organization's environment and requirements, and the CSB has defined, as well as communicated, policies and procedures for the specified areas.

48 **FY23 Supplemental:** To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?
Defined (Level 2)

49 **FY24 Core:** How mature are the organization`s processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls?
Defined (Level 2)

Comments: The CSB has defined its processes for performing ongoing security control assessments; granting system authorizations, including developing and maintaining system security plans; and monitoring security controls for individual systems.

50 **FY24 Supplemental:** How mature is the organization`s process for collecting and analyzing ISCM performance measures and reporting findings?
Consistently Implemented (Level 3)

Comments: The CSB's process for collecting and analyzing ISCM performance measures and reporting findings is consistently implemented. The process is systemic and allows the automatic notification of potential threats or attempts to exploit attack vectors on the CSB network.

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

Comments: Based on the maturity level of the individual areas within the Detect – ISCM function, the domain/function is assessed as "Defined."

51.2 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 maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?
Based on the maturity level of the individual areas within Detect – ISCM Program, the domain/function is assessed as "Defined." We limited our testing to those questions with criteria added to the metric that would materially change our fiscal year 2023 response. For those metrics with documented policies, procedures, and strategies, we rated the CSB at Level 2 (Defined). However, we did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

Function 4: Respond – Incident Response

52 **FY24 Supplemental:** To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents?
Defined (Level 2)

Comments: The CSB's incident response policies, procedures, plans, and strategies have been defined and communicated across the organization.

53 **FY24 Supplemental:** To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined, communicated, and implemented across the organization?
Defined (Level 2)

Comments: The CSB has defined and communicated the structure of its incident response teams, the roles and responsibilities of incident response stakeholders, and the associated levels of authority and dependencies.

54 **FY24 Core:** How mature are the organization`s processes for incident detection and analysis?
Defined (Level 2)

Comments: The CSB has an automatic ticketing system for incident reporting, has defined a common threat vector taxonomy, and has developed incident-handling procedures for specific types of incidents, as appropriate. In addition, the CSB has defined its processes and supporting technologies for detecting, analyzing, and prioritizing incidents, including defining the types of precursors and indicators and how they are generated and reviewed.

55 **FY24 Core:** How mature are the organization`s processes for incident handling?
Defined (Level 2)

Comments: The CSB has defined its processes to eradicate components of an incident, mitigate any vulnerabilities that were exploited, and recover system operations.

56 **FY24 Supplemental:** To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner?
Defined (Level 2)

Comments: The CSB has defined its requirements for personnel to report suspected security incidents to the CSB's chief information officer within CSB-defined time frames. In addition, the CSB has defined its processes for reporting security incident information to the U.S. Computer Emergency Readiness Team and law enforcement.

57 **FY23 Supplemental:** To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support?
Consistently Implemented (Level 3)

58 **FY23 Supplemental:** To what extent does the organization use the following technology to support its incident response program?

- Web application protections, such as web application firewalls
- Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools
- Aggregation and analysis, such as security information and event management (SIEM) products
- Malware detection, such as antivirus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and serversecurity tools

Defined (Level 2)

59.1 Please provide the assessed maturity level for the agency's Respond - Incident Response function.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within the Respond – Incident Response function , the domain/function is assessed as “Defined.”

59.2 Provide any additional information on the effectiveness (positive or negative) of the organizations incident response 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 incident response program effective?
Based on the maturity level of the individual areas within Respond – Incident Response function, the domain/function is assessed as “Defined." We limited our testing to those questions with criteria added to the metric that would materially change our fiscal year 2023 response. For those metrics with documented policies, procedures, and strategies, we rated the CSB at Level 2 (Defined). However, we did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

Function 5: Recover – Contingency Planning

60 **FY23 Supplemental:** To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined, communicated, and implemented across the organization, including appropriate delegations of authority?
Consistently Implemented (Level 3)

61 **FY24 Core:** To what extent does the organization ensure that the results of business impact analyses (BIA) are used to guide contingency planning efforts?
Defined (Level 2)

Comments: The CSB's "Information System Contingency Plan" is defined and explains how the results of business impact analyses are used to guide contingency planning efforts.

62 **FY24 Supplemental:** To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?
Consistently Implemented (Level 3)

Comments: The CSB has consistently developed procedures to ensure that its processes for "Information System Contingency Plan" development, maintenance, and integration with other continuity areas have been defined and include the following phases: activation and notification, recovery, and reconstitution.

63 **FY24 Core:** To what extent does the organization perform tests/exercises of its information system contingency planning processes?
Consistently Implemented (Level 3)

Comments: The CSB consistently performs" Information System Contingency Plan" testing on a periodic basis and includes personnel from across the organization.

64 **FY24 Supplemental:** To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?
Defined (Level 2)

Comments: The CSB's "Information System Contingency Plan" has defined procedures to ensure that the CSB performs information system backup and storage, including the use of alternate storage and processing sites.

65 **FY23 Supplemental:** To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk-based decisions?
Defined (Level 2)

66.1 Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within the Recover – Contingency Planning function , the domain/function is assessed as "Defined."

66.2 Provide any additional information on the effectiveness (positive or negative) of the organizations contingency planning 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 contingency program effective?
Based on the maturity level of the individual areas within Recover – Contingency Planning function, the domain/function is assessed as "Defined." We limited our testing to those questions with criteria added to the metric that would materially change our fiscal year 2023 response. For those metrics with documented policies, procedures, and strategies, we rated the CSB at Level 2 (Defined). However, we did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

APPENDIX A: Maturity Model Scoring

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

Function	Core	FY23 Supplemental	FY24 Supplemental	FY24 Assessed Maturity	FY24 Effectiveness	Explanation
Identify	2.17	2.00	2.00	Defined (Level 2)	Effective	We assessed the effectiveness of the CSB's information security program at Level 2.
Protect	2.25	2.20	2.13	Defined (Level 2)	Effective	We assessed the effectiveness of the CSB's information security program at Level 2.
Detect	2.00	2.00	3.00	Defined (Level 2)	Effective	We assessed the effectiveness of the CSB's information security program at Level 2.
Respond	2.00	2.50	2.00	Defined (Level 2)	Effective	We assessed the effectiveness of the CSB's information security program at Level 2.
Recover	2.50	2.50	2.50	Defined (Level 2)	Effective	We assessed the effectiveness of the CSB's information security program at Level 2.

Function	Core	FY23 Supplemental	FY24 Supplemental	FY24 Assessed Maturity	FY24 Effectiveness	Explanation
Overall Maturity	**2.18**	**2.24**	**2.33**	Defined (Level 2)	Effective	The U.S. Environmental Protection Agency Office of Inspector General contracted SB and Company LLC to assess the five 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 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics."

Function 1A: Identify – Risk Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	4	2
Consistently Implemented (Level 3)	1	0
Managed and Measurable (Level 4)	0	0

Maturity Level	Core	Supplemental
Optimized (Level 5)	0	0
Calculated Rating:	**2.20**	**2.00**

Function 1B: Identify – Supply Chain Risk Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	1
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	**2.00**	**2.00**

Function 2A: Protect – Configuration Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	2	3
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	0	0

Maturity Level	Core	Supplemental
Optimized (Level 5)	0	0
Calculated Rating:	**2.00**	**2.00**

Function 2B: Protect – Identity and Access Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	1
Consistently Implemented (Level 3)	2	0
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	**2.67**	**2.00**

Function 2C: Protect – Data Protection and Privacy

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	2	2
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	0	0

Maturity Level	Core	Supplemental
Optimized (Level 5)	0	0
Calculated Rating:	**2.00**	**2.00**

Function 2D: Protect – Security Training

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	1
Consistently Implemented (Level 3)	0	1
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	**2.00**	**2.50**

Function 3: Detect – ISCM

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	2	0
Consistently Implemented (Level 3)	0	1
Managed and Measurable (Level 4)	0	0

Maturity Level	Core	Supplemental
Optimized (Level 5)	0	0
Calculated Rating:	**2.00**	**3.00**

Function 4: Respond – Incident Response

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	2	3
Consistently Implemented (Level 3)	0	0
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	**2.00**	**2.00**

Function 5: Recover – Contingency Planning

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	1
Consistently Implemented (Level 3)	1	1
Managed and Measurable (Level 4)	0	0

Maturity Level	Core	Supplemental
Optimized (Level 5)	0	0
Calculated Rating:	**2.50**	**2.50**

Appendix B

Status of CSB Corrective Actions for FY 2023 FISMA Audit Recommendations

This table details the OIG's analysis of the corrective actions that the CSB has implemented for the recommendations issued in OIG Report No. Report No. 24-P-0035, *The CSB Has Improved Its Information Security Program but Needs to Document Recovery Testing Results, Consistent with National Institute of Standards and Technology Guidelines*, dated April 29, 2024.

Recommendation		Corrective Action	OIG analysis of corrective action status
1	Formally document the disaster recovery testing scenarios and lessons learned results, consistent with National Institute of Standards and Technology guidelines.	**Implemented** The CSB is now documenting the Disaster Recovery testing scenarios used as well as the lessons learned during the test in order to improve their Disaster Recovery process. The CSB provided support on April 11, 2024.	Closed. Corrective action was completed on July 15, 2024.

Appendix C

CSB Response to Draft Report

U.S. Chemical Safety and Hazard Investigation Board

1750 Pennsylvania Avenue NW, Suite 910 | Washington, DC 20006
Phone: (202) 261-7600 | Fax: (202) 261-7650
www.csb.gov

Steve Owens
Chairperson

Sylvia E. Johnson, Ph.D.
Board Member

Catherine J.K. Sandoval
Board Member

April 3, 2025

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 2024* (Project No. OA-FY24-0097).

The CSB has made significant improvements to its Information Security Program, as the OIG's fiscal year 2023 FISMA audit of the CSB demonstrated. The CSB exceeded maturity level 2, Defined, for each of the nine FISMA metric domains during that audit. Although those improvements have been consistently in place and enforced since that time, as well as further enhanced, the OIG's draft report states that the CSB remains at the Defined level for the 2024 fiscal year. The CSB strongly believes that the agency has met the threshold for maturity level 3, Consistently Implemented, as the appropriate policies, procedures, and strategies are being consistently implemented by the agency.

The draft OIG report presents just a single recommendation: that the CSB "develop a process for designating and maintaining personnel in key roles (permanent and/or temporary) to ensure the continuity of essential information security functions including the availability to respond to FISMA inquiries." This recommendation is based on the assertion in the draft OIG report that "the CSB designated staff as a Deputy CIO but they were not authorized to provide FISMA related documentation in the CIO's absence".

The CSB has a mature information technology (IT) program that maintains personnel in key roles, including essential information security functions. The CSB's current Chief Information Officer (CIO) and an experienced IT Specialist, who is performing the functions of the Deputy CIO, are both available to respond to requests. Contrary to the implication in the draft OIG report, during last year's FISMA audit a specific deadline was not stated by the auditor for the requested information. Consequently, the requested information was provided once the CIO returned from leave and was available to review the materials to be provided. If the CSB had been made aware of the need to provide materials by a specific date, personnel were available to do so. Although the CSB disagrees with the premise underlying the recommendation, CSB personnel will ensure the continuity of essential information security functions, including being available to promptly respond to FISMA inquiries.

Regards,

ANDREW STADDON

Digitally signed by ANDREW STADDON
Date: 2025.04.03 16:39:42 -04'00'

Andrew Staddon
Chief Information Officer

Appendix D

Distribution

Chairperson
Senior Advisor and General Counsel
Board Members
EPA OIG Liaison
Director of Administration/Board Affairs
Information Technology Director/Chief Information Officer
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 the OIG's whistleblower protection webpage.

Contact us:

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

EPA OIG Hotline: OIG.Hotline@epa.gov

Web: epaoig.gov

Follow us:

X: @epaoig

LinkedIn: linkedin.com/company/epa-oig

YouTube: youtube.com/epaoig

Instagram: @epa.ig.on.ig

www.epaoig.gov