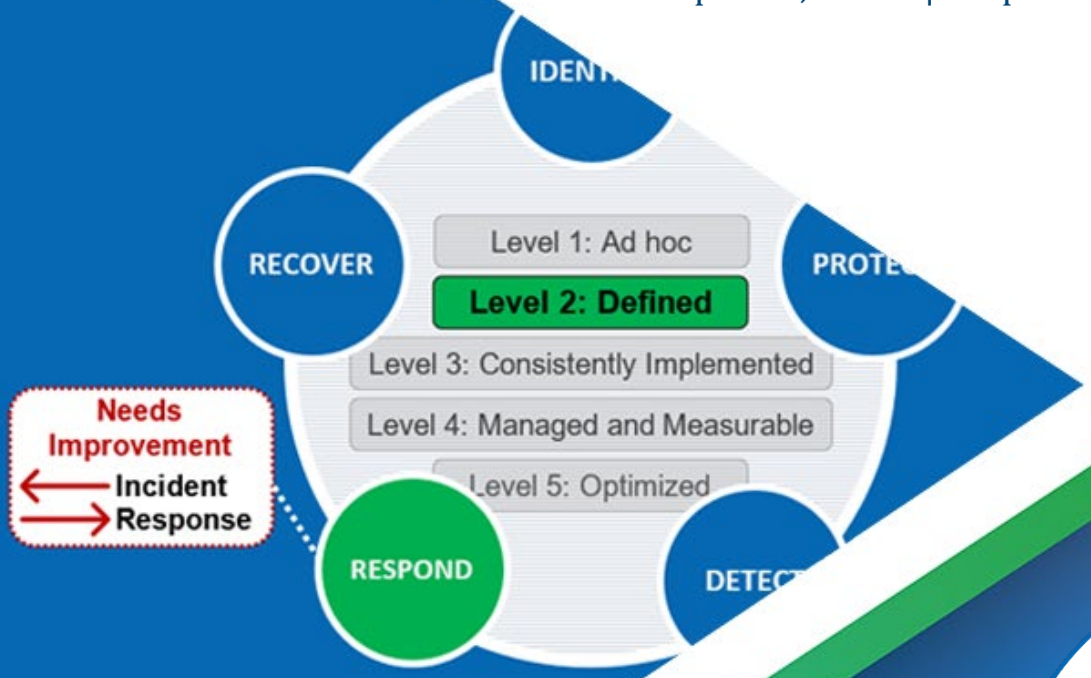
The CSB Has Improved Its Information Security Program but Needs to Document Recovery Testing Results, Consistent with National Institute of Standards and Technology Guidelines

April 29, 2024 | Report No. 24-P-0035



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

Inspectors general rate the maturity level of their agencies' information security programs. (EPA OIG image)

Are you aware of fraud, waste, or abuse in a CSB program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, D.C. 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG.Hotline@epa.gov

Learn more about our OIG Hotline.

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

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

24-P-0035
April 29, 2024

At a Glance

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

Why This Audit Was Performed

To accomplish this objective:

The U.S. Environmental Protection Agency Office of Inspector General conducted this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's compliance with the *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*. We contracted with SB & Company LLC to perform this audit under our direction and oversight.

The *FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* outlines five security function areas and nine corresponding domains to help federal agencies manage cybersecurity risks. The document also outlines five maturity levels by which inspectors general should rate their agencies' information security programs:

- Level 1, Ad-Hoc.
- Level 2, Defined.
- Level 3, Consistently Implemented.
- Level 4, Managed and Measurable.
- Level 5, Optimized.

To support this CSB mission-related goal:

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

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

List of OIG reports.

What SB & Company Found

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

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

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

Recommendations and Planned Agency Corrective Actions

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

Noteworthy Achievements

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

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

April 29, 2024

Andrew Staddon
Chief Information Officer
U.S. Chemical Safety and Hazard Investigation Board
1750 Pennsylvania Avenue NW, Suite 910
Washington, D.C. 20006

Dear Mr. Staddon:

This is a report on the U.S. Chemical Safety and Hazard Investigation Board's information security program. The report summarizes the results of information technology security work performed by SB & Company under the direction of the U.S. Environmental Protection Agency Office of Inspector General. This report also includes SB & Company's completed fiscal year 2023 Federal Information Security Management Act reporting template, as prescribed by the Office of Management and Budget. The project number for this evaluation is OA-FY23-0080.

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

Your staff provided acceptable corrective actions in response to the recommendation. The recommendation is resolved, and no final response to this report is required. 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 accessibility 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,

Sean W. O'Donnell
Inspector General

Table of Contents

Appendixes

Report of Independent Public Accountants

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

This report presents the results of our independent audit of the U.S. Chemical Safety and Hazard Investigation Board's information security program and practices. The Federal Information Security Modernization Act of 2014, or FISMA, requires federal agencies, including the CSB, to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluations to the Office of Management and Budget. The Office of Management and Budget has delegated its responsibility for the collection of annual FISMA responses to the U.S. Department of Homeland Security. The Department of Homeland Security, in conjunction with the Office of Management and Budget and the Council of the Inspectors General on Integrity and Efficiency, developed the fiscal year 2023–2024 *FISMA Reporting Metrics* to collect these responses. FISMA requires the agency inspector general or an independent external auditor to perform the independent evaluation as determined by the IG. The U.S. Environmental Protection Agency Office of Inspector General contracted SB & Company LLC to conduct this independent evaluation and monitored our work to ensure we met professional standards and contractual requirements.

We conducted our independent audit in accordance with Generally Accepted Government Auditing Standards and applicable American Institute of Certified Public Accountants standards.

The objective for this independent audit was to assess the effectiveness of the CSB's information security program and practices, including the CSB's compliance with FISMA and related information security policies, procedures, standards, and guidelines for October 1, 2022, to September 30, 2023. We based our work on a selection of CSB wide security controls and a selection of system specific security controls across CSB information systems. Additional details regarding the scope of our independent audit are included in the report's Background, Scope, and Methodology sections. Appendix A contains the FISMA matrix and Appendix B contains the status of prior year recommendations.

Consistent with applicable FISMA requirements, Office of Management and Budget policy and guidance, and National Institute of Standards and Technology standards and guidelines, the CSB established and maintained its information security program and practices for its information systems for the five cybersecurity functions and nine FISMA metric domains. Based on the results entered into CyberScope, we determined that the CSB's overall information security program was "Defined" because a majority of the FY 2023 FISMA core IG and FY 2023 metrics were rated Defined, or Level 2.

In our report, we have provided one finding and one recommendation to the chief information officer that, when addressed, should strengthen the CSB's information security program. The CSB chief information officer agreed with our finding and recommendation.

This independent audit did constitute an engagement in accordance with generally accepted government auditing standards. SB & Company did not render an opinion on the CSB's internal controls over financial reporting or over financial management systems as part of this audit. We caution that projecting the results of our audit to future periods or other CSB information systems not included in our selection is subject to the risk that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate.

Washington, D.C.
September 30, 2023

Table of Contents

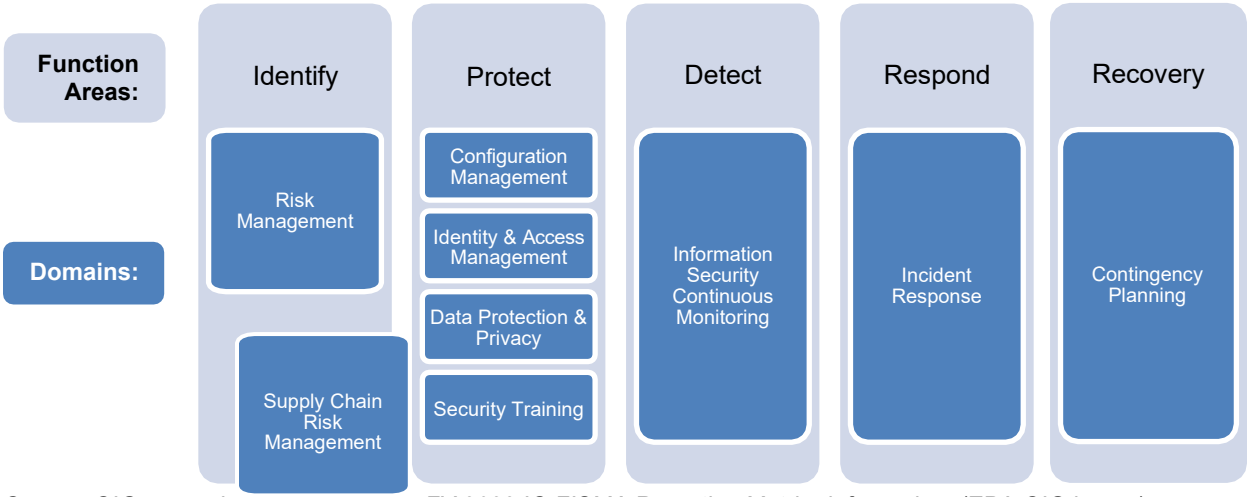
Appendix

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 U.S. Department of Homeland Security and the Office of Management and Budget issue an *IG FISMA Reporting Metrics* template for the inspector general, or IG, 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 40 metrics (20 core metrics and 20 metrics to be reviewed in FY 2023) 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, as shown in 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 2023 cybersecurity framework security function areas and domains



Source: OIG-created graphic based on *FY 2023 IG FISMA Reporting Metrics* information. (EPA OIG image)

The effectiveness of an agency's information security program is based on a five-tiered maturity model spectrum, as seen in 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

[1] The *Fiscal Year (FY) 2023 - 2024 FISMA Reporting 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 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 the National Institute of Standards and Technology to develop a voluntary framework based on existing standards, guidelines, and practices to reduce cyber risks to critical infrastructure.

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, which are 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 and mission needs.

Source: (*FY 2023 IG FISMA Reporting Metrics)*.

Scope and Methodology

SB & Company LLC conducted this audit from May to July 2023 in accordance with Generally Accepted Government Auditing Standards and applicable American Institute of Certified Public Accountants 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 Core IG Metrics Implementation Analysis and Guidelines*. We conducted a risk assessment of the FY 2023 IG FISMA metrics to determine whether changes made to the underlying criteria of the FISMA metric questions significantly changed since the FY 2022 evaluation.

We also evaluated the new FY 2023 criteria to assess whether they significantly changed the CSB's responses to the overall metric questions since the FY 2022 audit. We assessed each new criterion as either of these levels:

- 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 2022 audit for the identified metric question.

- Low Risk—The CSB made no significant changes to its information security program since the FY 2022 audit for the identified metric question.

We relied on responses to the FY 2022 CSB FISMA metric questions to answer the FY 2023 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. If the policies, procedures, and strategies were formalized and documented, we rated the agency at Level 2, Defined. If not, we rated the agency at Level 1, Ad Hoc.

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 on July 31, 2023.

Prior Reports

During our testing of the CSB's FY 2023 FISMA compliance, SB & Company followed up on deficiencies identified in the FY 2022 FISMA evaluation, as documented in Report No. 23-E-0016 titled ***The CSB Is at Increased Risk of Losing Significant Data as Vulnerabilities Are Not Identified and Remediated Timely***, dated May 2, 2023. We reported that the CSB lacked documented procedures and needed improvement in one domain**: Risk Management.** Specifically, SB & Company found that the CSB did not perform periodic vulnerability scanning, therefore failing to address identified vulnerabilities in a timely manner. The CSB completed the corrective actions. See Appendix B for more details on the status of corrective actions.

Results

As a result of the adoption of additional security processes, procedures, and strategies, the CSB has improved its overall maturity level to Level 2, Defined. 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: (SB & Company, *FY 2023 IG FISMA Reporting Metrics)*.

In FY 2023, the CSB continued to need improvements for a specific question in the "Incident Response" domain, as shown in Table 3. The National Institute of Standards and Technology (NIST) 800-34 revision 1: *Contingency Planning Guide for Federal Information Systems* states that all recovery and reconstitution events should be well documented, including an after-action report with lessons learned. Lessons learned are documented within the procedures that would establish the recovery of a system following a system disruption.

Table 3: CSB domains that require further improvement

Function area	Domain	FISMA questions that need improvement
Respond	Incident Response	The CSB has policies and procedures in place requiring disaster recovery testing. However, the disaster recovery testing scenarios and recording of the lessons learned during the test are not formally documented.

Source: SB & Company table.

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 hired a chief information officer in September 2022 and deputy chief information officer during FY 2023. The CIO and Deputy CIO have made significant progress in updating the CSB's information security program and have implemented new programs to address the prior year's concerns related to the overall effectiveness of the program.

Conclusion

National Institute of Standards and Technology guidelines provide that all disaster recovery testing events, including lessons learned, should be well documented within the Incident Response procedures. The CSB has policies and procedures in place requiring disaster recovery testing. However, the disaster recovery testing scenarios and recording of the lessons learned during the test are not formally documented. The CSB would adhere to NIST guidelines and strengthen its information security program's response time from a disruption by formally documenting the results of disaster recovery scenarios and lessons learned while testing those scenarios.

Recommendations

We recommend that the CSB Chief Information Officer:

Formally document the disaster recovery testing scenarios and lessons learned results, consistent with National Institute of Standards and Technology guidelines.

CSB Response and Procedures Performed

The CSB acknowledges the notice of recommendation. The CSB performed disaster recovery testing and annotated changes that need to be made, the CSB will establish a standard process to make it more formalized for future testing.

Status of Recommendations

RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date
1	8	Formally document the disaster recovery testing scenarios and lessons learned results, consistent with National Institute of Standards and Technology guidelines.	R	Chief Information Officer	April 15, 2024

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

Appendix A

Inspector General

Section Report

2023

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 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 Contingency Planning domain. Specifically, the CSB should document the lessons learned for disaster recover testing related to the Recover function area.

Function 1A: Identify – Risk Management

1. 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?
Defined (Level 2)

Comments : The CSB has a defined process to maintain a comprehensive inventory of its information systems. The information systems inventory is maintained and current.

2. 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. 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/taxonomy to develop and maintain an up-to-date inventory of software and licenses used in the organization's environment with the detailed information necessary for tracking and reporting. The inventory is maintained and current.

4. 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?

5. 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, as well as communicated, the policies, procedures, and processes that it uses to manage the cybersecurity risks associated with operating and maintaining its information systems.

6. 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?

7. 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)

Comments : The CSB's Information Technology Security Program has defined the roles and responsibilities of stakeholders involved in cybersecurity risk management and has communicated them across the organization.

8. 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)

Comments : The CSB implemented an information technology plan-of-action-and-milestone tracking sheet with defined time frames for remediating security weaknesses. It uses the tracking sheet to track identified security weaknesses until they are resolved.

9. 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)

Comments : The CSB has defined how cybersecurity risks are communicated in a timely and effective manner to the appropriate internal and external stakeholders.

10. 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 the appropriate internal and external stakeholders. Additionally, the CSB performs an annual risk assessment and measures its security posture against National Institute of Standards and Technology 800-53, Revision 5, dated September 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, 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 2022 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 1B: Identify – Supply Chain Risk Management

12. 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)

Comments : The CSB has procedures in place to manage the supply chain risks associated with the acquisition, maintenance, and disposal of systems, related components, and services through the exclusive use of vendors approved by the General Services Administration.

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

Comments : The CSB has procedures in place to manage supply-chain-risk-management activities at all levels in the organization.

14. 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?

15. 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 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 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 programs, the Identify function is assessed as "Defined." We limited our testing to those questions that would materially change our fiscal year 2022 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 the 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 2022 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 2A: Protect – Configuration Management

17. To what extent have the roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced?

18. 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?

19. 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)

Comments : The CSB's Configuration Management Policy defines its baseline configuration and component inventory policies and procedures.

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

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

21. 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-milestone tracking sheet for vulnerability management, which includes a time frame for remediating those vulnerabilities. The tracking sheet also includes documented procedures that define how it will be used to mitigate any identified security weaknesses.

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

Comments: The CSB has defined the Trusted Internet Connection, or TIC, program to assist in protecting its network.

23. 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?

24. 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)

Comments: The CSB's public website includes a link to the organization's Vulnerability Disclosure Policy.

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 2022 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. 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)

Comments: The CSB has defined an identity, credential, and access management, or ICAM, governance structure to align and consolidate the ICAM investments and monitoring programs, ensuring awareness and understanding. Additionally, the position of Information Technology Specialist has been filled.

27. 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)

Comments: The CSB consistently uses comprehensive policies and procedures for ICAM. The policies and procedures have been tailored to the organization's environment and include specific requirements. The CSB's Information Security Plan contains procedures for granting, changing, and removing access permissions. The CSB's Domain Password Policy activities are appropriately implemented.

28. 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?

29. 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)

Comments: The CSB has defined its processes for developing, documenting, and maintaining access agreements for individuals that access its systems.

30. 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?
Defined (Level 2)

Comments: The CSB implemented strong authentication mechanisms by using a virtual private network to remotely access the internal network. The CSB has defined controls for physical access to its local area network server room—specifically, electronic locks—and limits access permissions to appropriate personnel, accompanies visitors, and records access.

31. 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?
Defined (Level 2)

Comments : The CSB implemented strong authentication mechanisms by using a virtual private network to remotely access the internal network. The CSB has defined controls to limit physical access to its local area network server room—

specifically, electronic locks—and limits access permissions to appropriate personnel, accompanies visitors, and records access.

32. 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. 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)

Comments : The CSB has defined strong connection mechanisms by using a virtual private network to remotely access the internal network.

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 2022 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. 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)

Comments: The CSB has defined and communicated its privacy program plan and related policies and procedures for the protection of personally identifiable information that is collected, used, maintained, shared, and disposed of by its information systems. The CSB has determined the resources and optimal governance structure needed to effectively implement its privacy program.

36. 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. 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 network defenses.

38. To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events?

39. 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)

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 the 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 2022 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. 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)

Comments: The CSB has defined, as well as communicated, the roles and responsibilities for security awareness and training program stakeholders. For the CSB's information technology management program, security training is provided annually.

42. 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 assess the skills of the CSB's workforce, and is tailored to cover specific awareness and specialized security topics.

43. 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
Defined (Level 2)

Comments: The CSB uses a security awareness and training strategy/plan that annually leverages the CSB's organizational skills.

44. 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?

45. 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)?

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 2022 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. 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, or ISCM, strategy plan 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. 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)

Comments: The CSB has identified its ISCM stakeholders and defined their roles, responsibilities, levels of authority, and dependencies. The CSB has also communicated and implemented those roles and responsibilities across the organization.

49. 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. How mature is the organization`s process for collecting and analyzing ISCM performance measures and reporting findings?

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 the 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 2022 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. To what extent does the organization use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents?

53. 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?

54. 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. 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. 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?

57. 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)

Comments: The CSB has fully deployed the U.S. Department of Homeland Security's National Cybersecurity Protection System for intrusion detection/prevention capabilities for all traffic entering and leaving the organization's networks through a Trusted Internet Connection.

58. 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)

Comments: The CSB has identified and implemented technology to support the organization's incident response program.

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 the 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 2022 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. 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)

Comments: The CSB has consistently implemented the roles and responsibilities of stakeholders involved in information systems contingency planning and communicated these roles and responsibilities across the organization.

61. 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 defines how the results of business impact analyses are used to guide contingency planning efforts.

62. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?

63. To what extent does the organization perform tests/exercises of its information system contingency planning processes?
Defined (Level 2)

Comments: The CSB’s contingency plan testing is performed on a periodic basis and includes personnel from across the organization.

64. To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?

65. 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 teamsand used to make risk- based decisions?
Defined (Level 2)

Comments: The CSB has defined procedures to 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.

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 the 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 2022 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	FY23 Assessed Maturity	FY23 Effectiveness	Explanation
Identify	2.00	2.00	N/A	Defined (Level 2)		

Protect	2.00	2.10	N/A	Defined (Level 2)
Detect	2.00	2.00	N/A	Defined (Level 2)
Respond	2.00	2.50	N/A	Defined (Level 2)
Recover	2.00	2.50	N/A	Defined (Level 2)
Overall Maturity	**2.00**	**2.22**	**N/A**	

Function 1A: Identify – Risk Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	5	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 1B: Identify – Supply Chain Risk Management

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	2
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
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)	3	3
Consistently Implemented (Level 3)	0	1
Managed and Measurable (Level 4)	0	0
Optimized (Level 5)	0	0
Calculated Rating:	**2.00**	**2.25**

Function 2C: Protect – Data Protection and Privacy

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	2	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 2D: Protect – Security Training

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	1	2
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 3: Detect – ISCM

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	2	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 4: Respond – Incident Response

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	2	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 5: Recover – Contingency Planning

Maturity Level	Core	Supplemental
Ad Hoc (Level 1)	0	0
Defined (Level 2)	2	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**

Appendix B

Status of CSB Corrective Actions for Prior 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. 21-E-0071 *CSB's Information Security Program Is Not Consistently Implemented; Improvements Are Needed to Address Four Weaknesses,* dated February 9, 2021

Recommendation		Corrective Action	OIG analysis of corrective action status
1	Complete the Risk Assessment process as required by National Institute of Standards and Technology 800-37, re-evaluate the Risk Management Framework to make in more fluent to leverage day-to-day processes in place for completing the risk assessment, and determine how to best implement an organization wide governance process for monitoring and reporting on risks.	**Implemented** The CSB has completed a risk assessment and provided support of the assessment performed on June 1, 2023.	Corrective action completed. July 31, 2023
2	Document the process in place to monitor required flaw remediation to resolution and enhance the flaw remediation process to require approvals if risks cannot be mitigated to an acceptable level in a timely manner. In addition, develop timeframes and monitor the timeliness of applying patch updates.	**Implemented** The CSB has a documented procedure in place that defines how the tracking sheet will be used to mitigate any security weakness identified. The CSB provided support on June 1, 2023.	Corrective action completed. July 31, 2023
3	Perform disaster recovery testing on an annual basis. In addition, evaluate alternate methods to store backup media offsite.	**Implemented** Contingency plan tests for systems are now performed annually in conjunction with the annual March all-hands meeting to engage all users in the contingency plan testing. Additionally, based on the support provided by the CSB, backups are performed and moved to the cloud daily. The CSB provided support on March 31, 2023.	Corrective action completed. May 30, 2023

Appendix C

CSB Response to 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

March 20, 2024

Michelle Wicker, Program Manager
Office of Audit
Office of Inspector General
U.S. Environmental Protection Agency
Washington, DC 20004

Dear Ms. Wicker:

The Chemical Safety and Hazard Investigation Board (CSB) appreciates the opportunity to comment on the EPA Office of Inspector General's (OIG) draft report entitled, *The CSB Has Improved Its Information Security Program but Needs to Document Recovery Testing Results, Consistent with National Institute of Standards and Technology Guidelines* (Project No. OA-FY23-0080).

As the report recognizes, the CSB made significant improvements to its Information Security Program in FY 2023. As the report also recognizes, the CSB exceeded maturity level 2, Defined, for each of the nine metric domains in the Federal Information Security Modernization Act (FISMA). This is an especially significant achievement in a short period of time, given that the agency's information security program previously was designated as level 1, Ad Hoc. The CSB has continued to improve its information security program since the FY 2022 audit and expects to advance further in maturity level during the next audit period.

As the report acknowledges, since the FY 2022 audit, the CSB also has further developed its relationship with the Cybersecurity and Infrastructure Security Agency (CISA). The CSB has also been participating in interagency meetings and enrolling in new CISA offerings, such as Identity-as-a-Service to further improve agency security capabilities. The CSB now consistently ranks in the top quartile of compliant federal agencies for binding operational directives such as CISA BOD 18-01 (Email and Web Security). The CSB will continue to invest in its Information Security program and has already adopted many Zero Trust cybersecurity principles to further strengthen its information security.

The OIG's report presents a single recommendation: that the CSB formally document the results of lessons learned during its disaster-recovery scenarios. As the report acknowledges, the CSB conducted an agency-wide disaster recovery scenario and documented items to review and update to further improve agency recovery processes based on that exercise. Nevertheless, the CSB will ensure that the disaster recovery testing scenarios and lessons learned results are documented more formally going forward.

Additionally, the CSB will continue to strengthen such drills and will launch an agency-wide Emergency Alert app for CSB staff during FY 2024. These actions will further enhance the agency's disaster recovery program.

Finally, while the CSB appreciates that the report recognizes the significant progress that the agency has made under the direction of the CSB's Chief Information Officer (CIO) and Deputy CIO, the report incorrectly states that both joined the CSB during FY 2023. The CIO joined the CSB in September 2022. The Deputy CIO joined the CSB in June 2023.

Regards,

SABRINA MORRIS

Digitally signed by SABRINA MORRIS
Date: 2024.03.20 17:50:52 -04'00'

Sabrina Morris
Director of Administration

Appendix D

Distribution

Chairperson and Chief Executive Officer
Senior Advisor and General Counsel
EPA OIG Liaison
Information Technology Director/Chief Information Officer

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 Inquiries: OIG.CongressionalAffairs@epa.gov

Media Inquiries: OIG.PublicAffairs@epa.gov

EPA OIG Hotline: OIG.Hotline@epa.gov

Web: epaoig.gov

Follow us:

X (formerly Twitter): @epaoig

LinkedIn: linkedin.com/company/epa-oig

YouTube: youtube.com/epaoig

Instagram: @epa.ig.on.ig

www.epaoig.gov