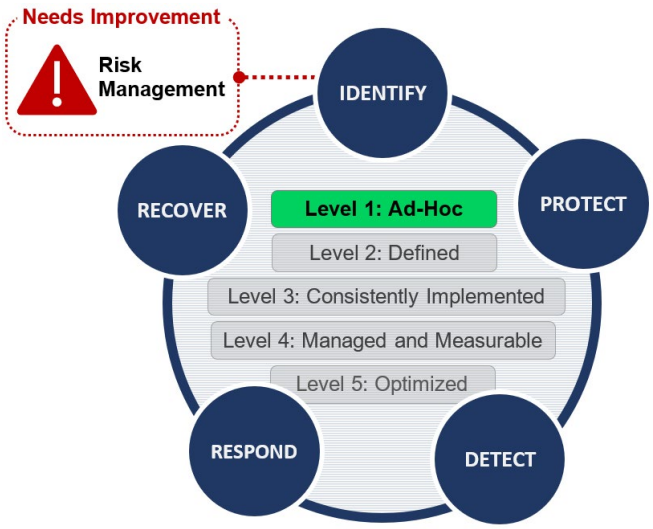
OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

CUSTOMER SERVICE ★ INTEGRITY ★ ACCOUNTABILITY

U.S. Chemical Safety Board

The CSB Is at Increased Risk of Losing Significant Data as Vulnerabilities Are Not Identified and Remediated Timely

Report No. 23-E-0016 **May 2, 2023**



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
OIG	Office of Inspector General

Cover Image: The U.S. Chemical Safety and Hazard Investigation Board's FY 2022 maturity levels by which inspectors general should rate their agencies' information security programs and the associated domains. (EPA OIG image)

Are you aware of fraud, waste, or abuse in an EPA or 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.epa.gov/oig

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

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

23-E-0016
May 2, 2023

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

Why This Evaluation Was Done

To accomplish this objective:

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

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

The reporting instructions outline five security function areas and nine corresponding domains to help federal agencies manage cybersecurity risks. The document also outlines five maturity levels by which inspectors general should rate their agencies' information security programs:

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

To support this CSB mission-related effort:

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

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

List of OIG reports.

What SB & Company Found

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

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

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

Recommendations and Planned Agency Corrective Actions

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

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

THE INSPECTOR GENERAL

May 2, 2023

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 2021 Federal Information Security Management Act reporting template, as prescribed by the Office of Management and Budget. The project number for this evaluation is OA-FY22-0136. This evaluation was conducted in accordance with *Quality Standards for Inspection and Evaluation*, published in January 2012 by the Council of the Inspectors General on Integrity and Efficiency.

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 recommendations. All recommendations are 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.epa.gov/oig.

Sincerely,

Sean W. O'Donnell

Table of Contents

SB & Company Report 1

CSB Response 8

Status of Recommendations 9

Appendixes

A SB & Company – Completed Department of Homeland Security CyberScope Template 10
B Status of CSB Corrective Actions for FY 2020 and FY 2021 FISMA Evaluation Recommendations 39
C CSB Response to Report 42
D Distribution 44

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 evaluation of the U.S. Chemical Safety and Hazard Investigation Board (CSB)'s information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including 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 (OMB). OMB has delegated its responsibility for the collection of annual FISMA responses to the Department of Homeland Security (DHS). DHS, in conjunction with OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), developed the Fiscal Year (FY) 2022 FISMA Reporting Metrics to collect these responses. FISMA requires the agency Inspector General (IG) 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 (OIG) contracted SB & Company, LLC (SBC) to conduct this independent evaluation and monitored our work to ensure we met professional standards and contractual requirements.

We conducted our independent evaluation in accordance with CIGIE Quality Standards for Inspection and Evaluation and applicable American Institute of Certified Public Accountants (AICPA) standards.

The objective for this independent evaluation was to assess the effectiveness of CSB's information security program and practices, including CSB's compliance with FISMA and related information security policies, procedures, standards, and guidelines for the period October 1, 2021, to September 30, 2022. 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 evaluation are included in the report's Background, Scope, and Methodology sections. Appendix A contains the CyberScope Template and Appendix B the status of prior year recommendations.

Consistent with applicable FISMA requirements, OMB policy and guidance, and National Institute of Standards and Technology (NIST) standards and guidelines, 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 CSB's overall information security program was "Ad Hoc" because a majority of the FY 2022 FISMA core IG metrics were rated Ad Hoc (Level 1). We reported a current year deficiency impacting a specific CyberScope question in Identify (risk management). Additionally, we issued, to the EPA OIG, a memo to report specific deficiencies found during our review, not all related to the CyberScope questions.

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 agreed with our conclusion and recommendation (see Management Response, page 15).

This independent evaluation did not constitute an engagement in accordance with Generally Accepted Government Auditing Standards. SB & Company, LLC did not render an opinion on CSB's internal controls over financial reporting or over financial management systems as part of this evaluation. We caution that projecting the results of our evaluation 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.
January 20, 2023

Table of Contents

Background ---------- 1

Scope and Methodology ---------- 2

Prior Evaluation ---------- 4

Results ---------- 5

Conclusion ---------- 7

Recommendation ---------- 7

Appendix

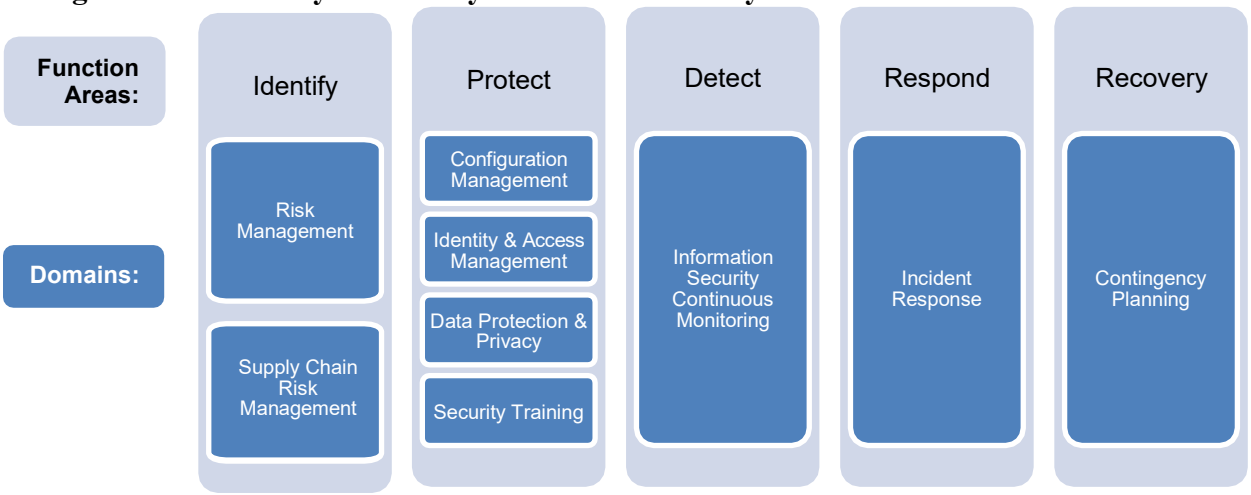
A SB & Company - Completed Department of Homeland Security CyberScope Template ---------- 10

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 *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*,[1] which can be found in Appendix A, provides 20 core metrics 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 2022 cybersecurity framework security function areas and domains



Source: OIG-created graphic based on *FY 2022 IG FISMA Reporting Metrics* information.

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

[1] *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*. 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.

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 2022 IG FISMA Reporting Metrics*.

Scope and Methodology

SB & Company, LLC (SBC or We) conducted this evaluation from May to July 2022 in accordance with CIGIE Quality Standards for Inspection and Evaluation and applicable American Institute of Certified Public Accountants (AICPA) standards.

During our evaluation, we assessed whether the CSB exceeded Maturity Level 2, *Defined*[3], for each of the 66 questions for the nine domains in the *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*. We conducted a risk assessment of the FY 2022 IG FISMA metrics to determine whether changes made to the underlying criteria of the FISMA metric questions significantly changed since the FY 2021 evaluation.

We also evaluated the new FY 2022 criteria to assess whether they significantly changed the CSB's responses to the overall metric questions since the FY 2021 evaluation. We assessed each new criterion as either:

[3] In FY2021 and 2020, the CSB's Maturity Level was Level 2, Defined. At the start of our evaluation, we thought the CSB had maintained their policies and procedures and had addressed any additional corrective actions.

- 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 2021 evaluation for the identified metric question.

- Low Risk—The CSB made no significant changes to its information security program since the FY 2021 evaluation for the identified metric question.

We relied on the responses to the FY 2021 CSB FISMA metric questions to answer the FY 2022 metric questions rated as *low risk*, and we conducted additional evaluation work to answer the questions rated as *high risk*.

We limited our assessment to determine whether the agency possessed the appropriate 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 evaluation results for each function area of the *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*.

Appendix A provides the OIG response to each FISMA metric, as submitted to the Office of Management and Budget on July 31, 2022.

Prior Evaluation

During our testing of the CSB's FY 2022 FISMA compliance, we followed up on deficiencies identified in the FY 2021 FISMA evaluation, as documented in Report No. 22-E-0025, CSB Is at Increased Risk of Losing Significant Data and Is Vulnerable to Exploitation, dated March 29, 2022. We reported that the CSB lacked documented procedures and needed improvement in two domains: (1) "Configuration Management" and (2) "Contingency Planning". Specifically, SB & Company, LLC found that the CSB did not:

1. Develop, adopt, and publish a Vulnerability Disclosure Policy (VDP) on its public facing websites to provide ethical hackers instruction on how to report vulnerabilities that they have identified and promote cooperation between internal and external stakeholders pertaining to vulnerabilities.
2. Resume the storage of system backups at an offsite location a sufficient distance from its headquarters that was discontinued during the COVID-19 pandemic.

The CSB completed corrective actions to address finding 1 listed above. The CSB did not complete corrective actions to address finding 2 listed above. See Appendix B for more details on the status of these corrective actions.

Results

The CSB's information security program achieved an overall maturity level of Level 1 (*Ad hoc*). This means that the CSB policies, procedures, and strategies are not formalized, and activities are performed in an Ad-Hoc, reactive manner. While the SB & Company assessed the effectiveness of the CSB's information security program at Level 2 (*Defined*), the FY 2022 Core IG Metrics Implementation Analysis and Guidelines directs OIGs to consider specific core metrics when assigning the calculated maturity level for the CyberScope scoring. Because the core questions of the FY 2022 metrics were rated Level 1, the CSB's overall calculated maturity level resulted in a Level 1 CyberScope rating.is assessed overall at the 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 1, *Ad-Hoc*
Identify	Supply Chain Risk Management	Level 1, *Ad-Hoc*
Protect	Configuration Management	Level 2, *Defined*
Protect	Identity and Access Management	Level 1, *Ad-Hoc*
Protect	Data Protection and Privacy	Level 2, *Defined*
Protect	Security Training	Level 1, *Ad-Hoc*
Detect	Information Security Continuous Monitoring	Level 2, *Defined*
Respond	Incident Response	Level 2, *Defined*
Recover	Contingency Planning	Level 2, *Defined*

Source: *FY 2022 IG FISMA Reporting Metrics*.

However, in FY 2022, 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	The CSB has policies and procedures in place, requiring monthly vulnerability scanning. However, due to staffing issues, monthly vulnerability scanning was discontinued in FY2022.

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. However, because of the shortened reporting period, only specific core metrics were considered when assigning the calculated maturity level. The core metrics included in the calculated assessment are highlighted in blue in Appendix A. Due to this, there

is a difference between the assessed and calculated maturity levels and resulted in an Ad-Hoc CyberScope[4] rating.

[4] CyberScope is a web-based application that collects data from each federal agency, to assess IT security. CyberScope relies on live data feeds and data entry by agency staff.

Conclusion

The CSB could improve and strengthen its cybersecurity program by resuming monthly vulnerability scanning. Vulnerability scanning will allow the CSB to identify and remediate vulnerabilities in a timely manner and decrease their risk of loss of data or disruption to agency operations.

Recommendation

We recommend that the Chief Information Officer for the U.S. Chemical Safety and Hazard Investigation Board:

1. Resume monthly vulnerability scanning and address identified vulnerabilities that put the confidentiality, integrity, and availability of CSB's data at risk in a timely manner.

CSB Response and Procedures Performed

The CSB agrees with the recommendation to resume vulnerability scanning and track vulnerabilities until resolution. The CSB will re-establish periodic vulnerability scanning by February 28, 2023 and track high-priority vulnerabilities until resolution. See Appendix C for the CSB's full response to the SB & Company LLC evaluation.

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	14	Resume vulnerability scanning and address identified vulnerabilities that put the confidentiality, integrity, and availability of CSB's data at risk in a timely manner.	C	Chief Information Officer	Feb 28, 2023	

[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 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 the SB & Company.

Inspector General

Section Report

2022

IG Annual

Chemical Safety Board

Function 0: Overall

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

Not Effective

0..2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

The U.S. Chemical Safety and Hazard Investigation Board's Information Security Program has demonstrated that it has defined policy, procedures, and strategies for all five of its information security function areas. The Office of Inspector General contracted SB & Company, LLC, to assess the five Cybersecurity Framework function areas and concluded that the CSB has achieved a Level 2, "Defined," which denotes that the CSB has defined policies, procedures, and strategies in adherence to the Fiscal Year 2022 Inspector General Federal Information Security Modernization Act, or FISMA, Reporting Metrics. While the CSB has policies, procedures and strategies defined for these function areas and many of the domains, improvements are still needed in the Risk Management and Supply Chain Management domains. Due to its size and limited resources, the CSB has not maintained a current, comprehensive, and accurate inventory of its information systems; performed a risk assessment in last 12 months; or documented processes related to supply chain risk management.

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? (NIST SP 800-53, Rev. 5: CA-3 and PM-5; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2022 CIO FISMA Metrics: 1.1-1.1.5, 1.3; OMB A-130, NIST SP 800-37, Rev.2: Task P-18; NIST 800-207, Section 7.3; EO 14028, Section 3; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B and D (5); CISA Cybersecurity & Incident Response Playbooks)

Ad Hoc (Level 1)

Comments: **The CSB has a defined process to maintain comprehensive inventory of its information systems; however, the inventory is not maintained and is not 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? (NIST SP 800-53, Rev. 5: CA-7, CM-8, CM-10, and CM-11; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2022 CIO FISMA Metrics: 1.3 and 4.0; OMB M-21-30; EO 14028, Section 4; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CSF: ID.AM-2; NIST SP 800- 37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 2)

Function 1A: Identify - Risk Management

Ad Hoc (Level 1)

Comments: The CSB has defined a process for using standard data elements/taxonomy to develop and maintain an up to date inventory: however, the inventory is not maintained and is not current.

3. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of software 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? (NIST SP 800-53, Rev. 5: CA-7, CM-8, CM-10, and CM-11; NIST SP 800-137; NIST IR 8011; FEA Framework, v2; FY 2022 CIO FISMA Metrics: 1.3 and 4.0; OMB M-21-30; EO 14028, Section 4; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section B; CSF: ID.AM-2; NIST SP 800- 37, Rev. 2: Task P-10 and P-16; NIST 800-207, Section 7.3; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8: Control 2)

Ad Hoc (Level 1)

Comments: The CSB has defined a process for using standard data elements/taxonomy to develop and maintain an up to date inventory of software assets and licenses utilized in the organization's environment with the detailed information necessary for tracking and reporting; however, the inventory is not maintained and is not 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 (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM-11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2022 CIO FISMA Metrics: 1.1; OMB M-19-03; NIST SP 800-37, Rev. 2: Task C-2, C-3, P-12, P-13, S-1 – S-3)?

Defined (Level 2)

Comments: The CSB Information System Contingency Plan has 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? (NIST SP 800-39; NIST SP 800-53, Rev. 5: RA-3 and PM-9; NIST IR 8286; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; OMB M-17-25; NIST SP 800-37 (Rev. 2): Tasks P2, P-3, P-14, R-2, and R-3)

Defined (Level 2)

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

Function 1A: Identify - Risk Management

6. To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (Federal Information Technology Acquisition Reform Act (FITARA), NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2) Task P-16; OMB M-19-03; OMB M-15-14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?
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. To what extent have roles and responsibilities of internal and external stakeholders involved in cyber security risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1, 2.3.2, and Appendix D; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; NISTIR 8286, Section 3.1.1, OMB A-123;; NIST SP 800-37 (Rev. 2) Section 2.8 and Task P-1; OMB M-19-03)?
Defined (Level 2)

Comments: The CSB IT 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 utilized for effectively mitigating security weaknesses (NIST SP 800-53 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2) Task A-6, R-3; OMB M-19-03, CSF v1.1, ID.RA-6)?
Ad Hoc (Level 1)

Comments: The CSB implemented an IT POA&M tracking sheet with defined timeframes for remediating security weaknesses; however, the organization discontinued use of the tracking sheet to identify and address security weaknesses.

9. To what extent does the organization ensure that information about cyber security risks is communicated in a timely manner to all necessary internal and external stakeholders (OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; NIST SP 800-37 (Rev. 2) Task M-5; SECURE Technology Act: s. 1326, NISTIR 8286)?
Defined (Level 2)

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

Function 1A: Identify - Risk Management

10. To what extent does the organization utilize 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? (NIST SP 800-39; OMB A-123; NIST IR 8286; CISA Zero Trust Maturity Model, Pillars 2-4, NIST 800-207, Tenets 5 and 7; OMB M-22-09, Federal Zero Trust Strategy, Security Orchestration, Automation, and Response)

Ad Hoc (Level 1)

Comments: While a risk assessment process is in place, however a risk assessment has not been performed in the last 12 months.

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 concluded as "Defined."

11.2. Provide any additional information on the effectiveness (positive or negative) of the organization's 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 and Supply Chain Risk Management domains, the Identify function is assessed as "Ad Hoc." We limited our testing to those questions that would materially change our FY 2021 response. For those metrics whose policies, procedures, and strategies were not documented, we rated the CSB at Level 1, "Ad Hoc." 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 utilize supply chain risk management policies and procedures to manage SCRM activities at all organizational tiers (NIST SP 800-37 Rev. 2, Section 2.8, NIST 800-53, SR-1, NIST CSF v1.1, ID.SC-1, NIST 800-161)?
Ad Hoc (Level 1)

Comments: Due to the size and resources of the organization, processes related to supply chain risk management are not formally documented.

13. To what extent does the organization utilize a supply chain risk management plan(s) to ensure the integrity, security, resilience, and quality of services, system components, and systems (OMB A-130, NIST SP 800-37 Rev. 2, Section 2.8, NIST 800-53, SR-2, SR-3; NIST 800-161, section 2.2.4 and Appendix E)?
Ad Hoc (Level 1)

Comments: Due to the size and resources of the organization, processes related to supply chain risk management are not formally documented.

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? (The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53, Rev. 5: SA-4, SR-3, SR-5 and SR-6 (as appropriate); NIST SP 800-152; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4, NIST IR 8276, NIST800-218, Task PO.1.3; FY 2022 CIO FISMA Metrics: 7.4.2; CIS Top 18 Security Controls v.8: Control 15)
Ad Hoc (Level 1)

Comments: Due to the size and resources of the organization, processes related to supply chain risk management are not formally documented.

15. To what extent does the organization maintain and monitor the provenance and logistical information of the systems and system components it acquires? (NIST SP 800-53 REV. 5: SR-4 and NIST SP 800-161, Provenance (PV) family)?
Ad Hoc (Level 1)

Comments: Due to the size and resources of the organization, processes related to supply chain risk management are not formally documented.

Function 1B: Identify - Supply Chain Risk Management

16.1. Please provide the assessed maturity level for the agency's Identify - Supply Chain Risk Management program.
Ad Hoc (Level 1)

Comments: Based on the maturity level of the individual areas within Supply Chain Risk Management, the domain is concluded as "Ad Hoc."

16.2. Please provide the assessed maturity level for the agency's Identify Function.
Ad Hoc (Level 1)

Comments: The maturity level of the individual areas within the Risk Management and Supply Chain Risk Management domains, identify function are assessed as "Ad Hoc." We limited our testing to those questions that would materially change our FY 2021 response. For those metrics whose policies, procedures, and strategies were not documented, we rated the CSB at Level 1, "Ad Hoc." However, we did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.

16.3. Provide any additional information on the effectiveness (positive or negative) of the organization's Supply Chain Risk Management domains, 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 and Supply Chain Risk Management domains, the Identify function is assessed as "Ad Hoc." We limited our testing to those questions that would materially change our FY 2021 response. For those metrics whose policies, procedures, and strategies were not documented, we rated the CSB at Level 1, "Ad Hoc." 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 across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: Section 2.4)?
Defined (Level 2)

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

Function 2A: Protect - Configuration Management

18. To what extent does the organization utilize 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 (NIST SP 800-128: Section 2.3.2; NIST SP 800-53 REV. 4: CM-9)?

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, or SDLC.

19. To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53 REV. 4: CM-2 and CM-8; FY 2022 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?

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 utilize settings/common secure configurations for its information systems? (NIST SP 800-53, Rev. 5: CM-6, CM-7, and RA-5; NIST SP 800-70, Rev. 4; FY 2022 CIO FISMA Metrics, Section 7, Ground Truth Testing; EO 14028, Section 4, 6, and 7; OMB M-22-09, Federal Zero Trust Strategy, Section D; OMB M - 22-05; CISA Cybersecurity & Incident Response Playbooks; CIS Top 18 Security Controls v.8, Controls 4 and 7; CSF: ID.RA-1 and DE.CM-8)

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 utilize flaw remediation processes, including patch management, to manage software vulnerabilities? (EO 14028, Sections 3 and 4; NIST SP 800-53, Rev. 5: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; NIST 800-207, section 2.1; CIS Top 18 Security Controls v.8, Controls 4 and 7; FY 2022 CIO FISMA Metrics: Section 8; CSF: ID.RA-1; DHS Binding Operational Directives (BOD) 18-02, 19-02, and 22-01; OMB M-22-09, Federal Zero Trust Strategy, Section D; CISA Cybersecurity Incident and Vulnerability Response Playbooks)

Ad Hoc (Level 1)

Comments: The CSB has an IT POA&M tracking sheet for patch management (including a timeframe for the remediation of security weaknesses) that is not used. Additionally, there is not a documented procedure in place that defines how the tracking sheet will be used to mitigate any security weaknesses identified.

Function 2A: Protect - Configuration Management

22. To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26)?
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, as appropriate (NIST SP 800-53 REV. 4: CM-2, CM-3 and CM-4; CSF: PR.IP-3).
Defined (Level 2)

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

24. To what extent does the organization utilize a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet-accessible federal systems (OMB M-20-32 and DHS BOD 20-01)?
Defined (Level 2)

> Comments: The CSB's website indicates that a Vulnerability Disclosure Policy has been published to the pubic facing website.

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 Configuration Management, the domain is concluded as "Defined."**

25.2. Provide any additional information on the effectiveness (positive or negative) of the organization's 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?

Function 2A: Protect - Configuration Management

Based on the maturity level of the individual areas within Configuration Management, the domain is assessed as "Defined." We limited our testing to those questions with criteria added to the metric that would materially change our FY 2021 response. If the policies, procedures, and strategies were documented, 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 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 across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; NIST SP 800-63-3 and 800-63A, B, and C; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM), OMB M-19-17)?

Ad Hoc (Level 1)

Comments: The CSB has defined an ICAM governance structure to align and consolidate the ICAM investments and monitoring programs, ensuring awareness, and understanding. However, the position of IT Specialist has not been filled for approximately 11 months.

27. To what extent does the organization utilize a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities (FICAM, OMB M-19-17; NIST SP 800-53 REV. 4: AC-1 and IA-1; OMB M-19-17, Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

Consistently Implemented (Level 3)

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

Function 2B: Protect - Identity and Access Management

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 (NIST SP 800-53 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11, OMB M-19-17)?

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 for rescreening individuals on a periodic basis.

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 (NIST SP 800-53 REV. 4: AC-8, PL-4, and PS-6)?

Ad Hoc (Level 1)

Comments: The CSB has defined its processes for developing, documenting, and maintaining access agreements for individuals that access its systems. However, evidence was not provided to show that the Computer Security Employee Acknowledgment form is still utilized.

30. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for nonprivileged users to access the organization's facilities [organization defined entry/exit points], networks, and systems, including for remote access? (EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; OMB M19-17, NIST SP 800-157; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6)

Ad Hoc (Level 1)

Comments: The CSB implemented strong authentication mechanisms in the use of a virtual private network, or VPN, to remotely access the internal network. However, the CSB did not define that the process was still in use. The CSB has defined controls for physical access to their local area network, or LAN, server room using electronic locks, limiting access permissions to appropriate personnel, and accompanying visitors and recording their access.

Function 2B: Protect - Identity and Access Management

31. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access? (EO 14028, Section 3; HSPD-12; NIST SP 800-53, Rev. 5: AC-17 and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63 and 800-157; OMB M-19-17; FY 2022 CIO FISMA Metrics: Section 2; OMB M-22-05; OMB M-22-09, Federal Zero Trust Strategy, Section A (2); CSF: PR.AC-1 and 6; DHS ED 19-01; NIST 800-207 Tenet 6; CIS Top 18 Security Controls v.8: Control 6)

Ad Hoc (Level 1)

Comments: The CSB implemented strong authentication mechanisms in the use of a VPN to remotely access the internal network. However, the CSB did not define that the process was still in use. CSB has defined controls to limit physical access to their LAN server room using electronic locks, limiting access permissions to appropriate personnel, and accompanying visitors and recording their 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? (EO 14028, Section 8; FY 2022 CIO FISMA Metrics: 3.1; OMB M-21-31; OMB M-19-17; NIST SP 800-53, Rev. 5: AC-1, AC2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; DHS ED 19-01; CSF: PR.AC-4; CIS Top 18 Security Controls v.8: Controls 5, 6, and 8)

Defined (Level 2)

Comments: 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 access sessions (NIST SP 800-53 REV. 4: AC-11, AC-12, AC-17, AC-19, AU-2, IA-7, SC-10, SC-13, and SI-4; CSF: PR.AC-3; and FY 2022 CIO FISMA Metrics: 2.10 and 2.11).

Ad Hoc (Level 1)

Comments: The CSB has defined strong connection mechanisms in the use of a VPN to remotely access the internal network. However, evidence was not provided at the time of the review that the VPN was still in use.

Function 2B: Protect - Identity and Access Management

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 Identity and Access Management, the domain is concluded as "Defined."

34.2. Provide any additional information on the effectiveness (positive or negative) of the organization's 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, the domain is assessed as "Defined." We limited our testing to those questions with criteria added to the metric that would materially change our FY 2021 response. For those metrics whose policies, procedures, and strategies were documented, 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 (NIST SP 800-122; NIST SP 800-37 (Rev. 2) Section 2.3, Task P-1 ; OMB M-20-04; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J, FY 2020 SAOP FISMA metrics, Sections 1 through 4, 5(b))?

Defined (Level 2)

Comments: The CSB has defined and communicated its privacy program plan and related policies and procedures for the protection of PII that is collected, used, maintained, shared, and/or 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 has the organization implemented the encryption of data rest, in transit, limitation of transference of data by removable media, and sanitization of digital media prior to disposal or reuse to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (EO 14028, Section 3(d); OMB M-22-09, Federal Zero Trust Strategy; NIST 800-207; NIST SP 800-53, Rev. 5; SC-8, SC28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2022 CIO FISMA Metrics: 2.1, 2.2, 2.12, 2.13; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6; CIS Top 18 Security Controls v. 8: Control 3)

Function 2C: Protect - Data Protection and Privacy

Defined (Level 2)

Comments: The CSB's policies and procedures have been defined and communicated for the encryption of data at rest, 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 PII 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 to prevent data exfiltration and enhance network defenses? (FY 2022 CIO FISMA Metrics, 5.1; NIST SP 800-53, Rev. 5: SI3, SI-7, SI-4, SC-7, and SC-18; DHS BOD 18-01; DHS ED 19- 01; CSF: PR.DS-5, OMB M-21-07; CIS Top 18 Security Controls v.8: Controls 9 and 10)

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? (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2020 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25)?

Defined (Level 2)

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

39. To what extent does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53 REV. 4: AR-5, FY 2020 SAOP FISMA Metrics, Sections 9 10, and 11)

Ad Hoc (Level 1)

Comments: The CSB has defined its privacy awareness training program based on organizational requirements, culture, and the types of PII or protected health information, also known as PHI, that its users have access to; however, evidence was not provided as support that privacy training is held on a periodic basis. Additionally, the CSB has not developed role-based privacy training for individuals having responsibility for PII/PHI or activities involving PII/PHI.

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 Data Protection and Privacy, the domain is concluded as "Defined."

Function 2C: Protect - Data Protection and Privacy

40.2. Provide any additional information on the effectiveness (positive or negative) of the organization's 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 Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains, the Protect function is assessed as "Defined." We limited our testing to those questions with criteria added to the metric that would materially change our FY 2021 response. For those metrics whose policies, procedures, and strategies were documented, 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 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 security responsibilities (NIST SP 800-53 REV. 4: AT-1; and NIST SP 800-50).

Defined (Level 2)

Comments: The CSB has defined the roles and responsibilities for security awareness and training program stakeholders have been defined and communicated across the agency. For the CSB Information Technology management, security training is provided annually, and is published on the internal website; however, the CSB did not provide supporting evidence that security training was provided in the last 12 months.

42. To what extent does the organization utilize 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? (FY 2022 CIO FISMA Metrics, Section 6; NIST SP 800-53, Rev. 5: AT-2, AT-3, and PM-13; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS Top 18 Security Controls v.8: Control 14)

Ad Hoc (Level 1)

Comments: Security training is provided annually and is used to access the skills of the CSB's workforce and provide tailored awareness and specialized security training. While the program is documented, the CSB did not provide evidence during the review to support that security training was provided in the last 12 months.

Function 2D: Protect - Security Training

43. To what does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (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, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT-1).
Ad Hoc (Level 1)

Comments: The CSB utilizes a security awareness and training strategy/plan that leverages its organizational skills annually; however, it did not provide evidence that security training was provided in the last 12 months.

44. To what extent does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, 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 (NIST SP 800-53 REV. 4: AT-2; FY 2022 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).
Ad Hoc (Level 1)

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

45. To what extent does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800-53 REV. 4: AT-3 and AT-4; FY 2022 CIO FISMA Metrics: 2.15)?
Ad Hoc (Level 1)

Comments: Training for individuals in specialized IT support areas has not been conducted in the last 12 months.

46.1. Please provide the assessed maturity level for the agency's Protect - Security Training program.
Ad Hoc (Level 1)

Comments: Based on the maturity level of the individual areas within Security Training, the domain is concluded as “Ad Hoc.”

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

Function 2D: Protect - Security Training

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 Protection function is concluded as "Defined."

46.3. Provide any additional information on the effectiveness (positive or negative) of the organization's 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 Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains, the Protect function is assessed as "Defined." We limited our testing to those questions with criteria added to the metric that would materially change our FY 2021 response. For those metrics whose policies, procedures, and strategies were documented, 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 utilize information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier? (NIST SP 800-53, Rev. 5: CA-7, PM-6, PM-14, and PM-31; NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6; CIS Top 18 Security Controls v.8: Control 13)

Ad Hoc (Level 1)

Comments: The CSB ISCM strategy plan is tailored to the organization's environment and requirements, and those policies and procedures have been defined and communicated for the specified areas. However, the CSB did not provide evidence during the review to support that the ISCM policies are implemented.

48. To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; NIST 800-37, Rev. 2 Task P-7 and S-5)

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.

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? (OMB A-130; NIST SP 800-137: Section 2.2; NIST SP 800-53, Rev. 5: CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2) Task S-5; NIST SP 800-18, Rev. 1, NIST IR 8011; OMB M-14-03; OMB

Function 3: Detect - ISCM

M-19-03)

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 (NIST SP 800-137)?

Consistently Implemented (Level 2)

Comments: The CSB's process for collecting and analyzing ISCM performance measures and reporting findings is systemic and allows 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 domain/function.

Defined (Level 2)

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

51.2. Provide any additional information on the effectiveness (positive or negative) of the organization's 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, 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 FY 2021 response. For those metrics whose policies, procedures, and strategies were documented, 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 utilize an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents (NIST SP 800-53 REV. 4: IR-8; NIST SP 800-61 Rev. 2, section 2.3.2; CSF, RS.RP-1, Presidential Policy Directive (PPD) 8 – National Preparedness)?

Defined (Level 2)

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

Function 4: Respond - Incident Response

53. To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; CSF, RS.CO-1, OMB M-20-04; FY 2022 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

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. How mature are the organization's processes for incident detection and analysis? (EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4, IR-5, and IR-6; NIST SP 800-61 Rev. 2; OMB M20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and CIS Top 18 Security Controls v.8: Control 17)

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 and analyzing incidents—including the types of precursors and indicators and how they are generated and reviewed—and for prioritizing incidents.**

55. How mature are the organization's processes for incident handling? (EO 14028, Section 6; OMB M-22-05, Section I; CISA Cybersecurity Incident and Vulnerability Response Playbooks; FY 2022 CIO FISMA Metrics: 10.6; NIST 800-53, Rev. 5: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)

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 (FISMA; OMB M-20-04; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 5; DHS Cyber Incident Reporting Unified Message)

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 timeframes. In addition, the CSB has defined its processes for reporting security incident information to the United States Computer Emergency Readiness Team, or US-CERT, and law enforcement.

Function 4: Respond - Incident Response

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 (NIST SP 800-86; NIST SP 800-53 REV. 4: IR-4; OMB M-20-04; PPD-41).
Consistently Implemented (Level 3)

Comments: The CSB has fully deployed the U.S. Department of Homeland Security's Einstein program for intrusion detection/ prevention capabilities for all traffic entering and leaving the organization's networks through a Trusted Internet Connection, or TIC.

58. To what extent does the organization utilize 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 server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44)
Defined (Level 2)

Comments: The CSB has identified and fully defined its requirements for the incident response technologies it plans to utilize in the specified areas.

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

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

59.2. Provide any additional information on the effectiveness (positive or negative) of the organization's Incident Response program that was not noted in the questions above. Taking into consideration the 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, 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 FY 2021 response. For those metrics whose policies, procedures, and strategies were documented, 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 and communicated across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1, CP-2, and CP-3; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

Consistently Implemented (Level 3)

Comments: The CSB has consistently implemented the roles and responsibilities of stakeholders involved in information systems contingency planning and communicated them 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? (FY 2022 CIO FISMA Metrics: 10.1.4; NIST SP 800-53, Rev. 5: CP-2, and RA-9; NIST SP 800-34, Rev. 1, 3.2; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; CSF:ID.RA-4)

Defined (Level 2)

Comments: The CSB Information System Contingency Plan is defined and verified that 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 (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34; FY 2022 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

Defined (Level 2)

Comments: The CSB has defined procedures to ensure that CSB 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 To what extent does the organization perform tests/exercises of its information system contingency planning processes? (FY 2022 CIO FISMA Metrics: 10.1; NIST SP 800-34; NIST SP 800-53, Rev. 5: CP-3 and CP-4; CSF: ID.SC-5 and CSF: PR.IP10; CIS Top 18 Security Controls v.8: Control 11)

Ad Hoc (Level 1)

Comments: Processes for information system contingency plan testing/exercises have not been defined. Contingency plan testing has not been performed in the prior 12 months due to a lack of resources.

64 To what extent does the organization perform information system backup and storage, including use of alternate storage and

processing sites, as appropriate (NIST SP 800-53 REV. 4: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; aNIST CSF: PR.IP-4; FY 2022 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?

Function 5: Recover - Contingency Planning

Ad Hoc (Level 1)

Comments: CSB Information System Contingency Plan has defined procedures to ensure that the CSB performs information system backup and storage, including use of alternate storage and processing sites. However, the system backup to tape, which is the method used to move and store data offsite, is not regularly performed.

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 teams and used to make risk-based decisions (CSF: RC.CO-3; NIST SP 800-53 REV. 4: CP-2 and IR-4)?

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 domain/function.

Defined (Level 2)

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

66.2. Provide any additional information on the effectiveness (positive or negative) of the organization's Contingency Planning program that was not noted in the questions above. Taking into consideration the 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, 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 FY 2021 response. For those metrics whose policies, procedures, and strategies were documented, 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.

Summary

Cycle	Maturity Level	Mean	Mode
FY22 Core Metrics	Ad Hoc (Level 1)	1.49	Ad Hoc (Level 1)
FY22 Supplementary Metrics	Defined (Level 2)	1.86	Defined (Level 2)
FY22 Overall	Ad Hoc (Level 1)	1.49	Ad Hoc (Level 1)

Overall

Function	Calculated Maturity Level	Mean	Mode	Assessed Maturity Level	Explanation
Function 1: Identify – Risk Management / Supply Chain Risk Management	Ad Hoc (Level 1)	1.17	Ad Hoc (Level 1)	Ad Hoc (Level 1)	The maturity level of the individual areas within the Risk Management and Supply Chain Risk Management domains, Identify function are assessed as "Ad Hoc." We limited our testing to those questions that would materially change our FY 2021 response. For those metrics whose policies, procedures, and strategies were not documented, we rated the CSB at Level 1, "Ad Hoc." However, we did not test to determine what additional steps the CSB needs to complete to achieve a higher maturity level.
Function 2: Protect – Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Defined (Level 2)	1.54	Defined (Level 2)	Defined (Level 2)	
Function 3: Detect – ISCM	Defined (Level 2)	1.50	Defined (Level 2)	Defined (Level 2)	

Function 4: Respond – Incident Response	**Defined (Level 2)**	**2.22**	**Defined (Level 2)**	**Defined (Level 2)**
Function 5: Recover – Contingency Planning	**Defined (Level 2)**	**1.67**	**Defined (Level 2)**	**Defined (Level 2)**
Function 0: Overall	**Not Effective**	**1.49**	**Ad Hoc (Level 1)**	**Not Effective**

APPENDIX A: Maturity Model Scoring

Function 1A: Identify - Risk Management

Function	Count
Ad-Hoc	4
Defined	1
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Ad Hoc (Level 1)

Function 1B: Identify - Supply Chain Risk Management

Function	Count
Ad-Hoc	1
Defined	0
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Ad Hoc (Level 1)

APPENDIX A: Maturity Model Scoring

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	1
Defined	1
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Defined (Level 2)

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	2
Defined	1
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Ad Hoc (Level 1)

APPENDIX A: Maturity Model Scoring

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Defined (Level 2)

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	1
Defined	0
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Ad Hoc (Level 1)

APPENDIX A: Maturity Model Scoring

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	1
Defined	1
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Defined (Level 2)

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	1
Managed and Measurable	0
Optimized	0

Calculated Rating: Defined (Level 2)

APPENDIX A: Maturity Model Scoring

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	1
Defined	1
Consistently Implemented	0
Managed and Measurable	0
Optimized	0

Calculated Rating: Defined (Level 2)

Appendix B

Status of CSB Corrective Actions for FY 2020 and FY 2021 FISMA Evaluation Recommendations

The table below describes the recommendations from previous FISMA evaluations that remained unimplemented as of January 2023.

Recommendation	Corrective action	OIG analysis of corrective action
Complete the Risk Assessment process as required by NIST 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. OIG Report No. 21-E-0071, *CSB's Information Security Program Is Not Consistently Implemented; Improvements Are Needed to Address Four Weaknesses*, issued February 9, 2021	**Not Implemented** Based on follow-up discussions with the CSB information technology management, while a risk assessment process is in place, a risk assessment has not been performed since FY 2020 due to the ongoing effects of the coronavirus pandemic. In addition, due to the size and resources of the organization, processes related to governance and process management are handled through manual processes. There is no automated solution that provides a centralized, enterprisewide view of cybersecurity risks across the organization. However, there are documented procedures in place for implementing an organizationwide governance process for monitoring and reporting on risks.	Open: corrective action in process. Planned completion date: June 30, 2023. The CSB will perform a risk assessment by the end of the calendar year and establish it as a yearly process. Additionally, the CSB has procured a Security Information and Event Management System, which will enable it to have an automated solution to view cybersecurity risks across the organization. This will be implemented by the end of the calendar year and will be hosted on a FedRAMP Moderate GovCloud.
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 time frames and monitoring on the timeliness of applying patch updates. OIG Report No. 21-E-0071, *CSB's Information Security Program Is Not Consistently Implemented; Improvements Are Needed to Address Four Weaknesses*, issued February 9, 2021	**Implemented** The CSB reestablished periodic vulnerability scanning in February 2023 and the results of the scans are stored. Critical and high vulnerabilities are documented in the plan of actions and milestones tracking sheet until resolution.	Closed: corrective action completed.
Implement Information Security awareness and specialized security training policies and procedures to provide exposure to areas specific to individuals that have a role supporting	**Implemented** Based on discussions with the CSB information technology management, specialized security training is normally provided; however, training for individuals in	Closed: corrective action completed.

Recommendation	Corrective action	OIG analysis of corrective action
Information Security or technology related areas. In addition, document an Information Security awareness and training strategy that leverages its organizational skills assessment and factors the training program priorities, funding, the goals of the program, and targeted audiences. OIG Report No. 21-E-0071, *CSB's Information Security Program Is Not Consistently Implemented; Improvements Are Needed to Address Four Weaknesses*, issued February 9, 2021	specialized IT support areas has not been conducted since FY 2020.	
Perform disaster recovery testing on an annual basis. In addition, evaluate alternate methods to store backup media offsite. OIG Report No. 21-E-0071, *CSB's Information Security Program Is Not Consistently Implemented; Improvements Are Needed to Address Four Weaknesses*, issued February 9, 2021	**Not Implemented** Processes for information system contingency plan testing and exercises have not been defined. Contingency plan tests for systems are performed in an ad-hoc, reactive manner due to the continuing impact of the coronavirus pandemic and lack of resources. Additionally, based on discussions with the CSB information technology management, the backups are not being consistently rotated off-site.	Open: corrective action in process. Planned completion date: March 31, 2023. The CSB will establish contingency plan testing policies by the end of the calendar year and conduct testing at least once a year.
Develop and deploy a Vulnerability Disclosure Policy to formalize security feedback and to comply with Office of Management and Budget M-20-32 and U.S. Department of Homeland Security Binding Operational Directive 20-01. OIG Report No. 22-E-0025, *CSB Is at Increased Risk of Losing Significant Data and Is Vulnerable to Exploitation,* issued March 29, 2022.	**Implemented** The CSB has developed and deployed a Vulnerability Disclosure Policy to its public-facing website to formalize security feedback and comply with OMB M-20-32 and DHS BOD 20-01.	Closed: corrective action completed.
Immediately restore off-site storage of backup tapes and implement a strategy that will ensure that the Agency consistently stores backups of its systems at an off-site location. Additionally, explore alternative methods of off-site backup that can be performed automatically and do not require physical intervention by CSB	**Implemented** Off-site backups are consistently done daily.	Closed: corrective action completed.

Recommendation	Corrective action	OIG analysis of corrective action
personnel, such as storing backups in the cloud. OIG Report No. 22-E-0025, *CSB Is at Increased Risk of Losing Significant Data and Is Vulnerable to Exploitation,* issued March 29, 2022.		

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 14, 2023

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 Is at Increased Risk Of Losing Significant Data as Vulnerabilities Are Not Identified and Remediated Timely* (Project No. OA-FY22-0136).

The CSB notes that the report assesses the effectiveness of the CSB's information security program and practices for the period October 1, 2021, to September 30, 2022. As the OIG likely is aware, during virtually all this period, the CSB did not have a Chief Information Officer (CIO). Moreover, the CSB Chairperson in office during the vast majority of this time resigned and left the CSB in late July 2022. Upon the former Chairperson's departure, the two remaining members of the CSB Board immediately placed high priority on hiring a new CIO and addressing the CSB's cybersecurity and information technology infrastructure challenges (many of which have been documented in prior OIG reports).[1]

[1] The two remaining Board Members at the time were Sylvia E. Johnson, Ph.D., and Steve Owens. Member Owens was selected by the Board to be the CSB's Interim Executive Authority and was nominated by President Biden to be the new CSB Chairperson. Member Owens was confirmed as Chairperson by the U.S. Senate in December 2022. The current CSB Board Members are Chairperson Owens, Member Johnson, and Member Catherine J.K. Sandoval (who joined the Board in February 2023).

Beginning with the onboarding of the new CIO in September 2022, the CSB has proactively taken aggressive, concrete steps to improve the agency's cybersecurity posture. The new CSB CIO has a strong cybersecurity background, and upon joining the agency in September 2022, the new CIO and the Board immediately began working to prioritize and correct the CSB's IT deficiencies.

To that end, the CSB established a strong working relationship with the Cybersecurity and Infrastructure Security Agency (CISA), enrolling in several of CISA's programs, including the Vulnerability Disclosure Program (VDP) and the Continuous Diagnostics and Mitigation (CDM) Program. All CSB assets are now being scanned for vulnerabilities on a daily basis utilizing the cybersecurity tools provided by CISA, with ongoing remediation efforts leading to a dramatic improvement in the CSB's Federal Cyber Exposure Scorecard and much improved compliance with binding operational directives on cybersecurity. Additionally, several vulnerabilities were addressed through the VDP program for the CSB.gov website, with no current vulnerabilities reported. Through these and other ongoing efforts, CSB is demonstrating its strong commitment to cybersecurity.

Further, CSB established a Microsoft Azure cloud presence, which is now being utilized to perform daily backups of critical servers to an offsite location in another region. Virtual machines in that same cloud region are also configured and ready for continuity of operations and disaster recovery needs for the agency.

The CSB appreciates the work of the audit staff at the EPA OIG in connection with both this report and others produced in prior years that have focused on cybersecurity and IT issues at the CSB. As the efforts discussed above demonstrate, the CSB has been taking (and will continue to take) the actions needed to correct the deficiencies identified in this report, which (as noted) addresses practices through September 2022 and does not take into account the significant steps taken by the CSB since that time.

The OIG's report presents a single recommendation: that the CSB CIO resume the monthly vulnerability scanning and address identified vulnerabilities that put the confidentiality, integrity, and availability of CSB's data at risk in a timely manner. The CSB agrees with the recommendation, and as discussed, began doing this before receiving the OIG's report.

Sincerely,

Sabrina Morris
Acting 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