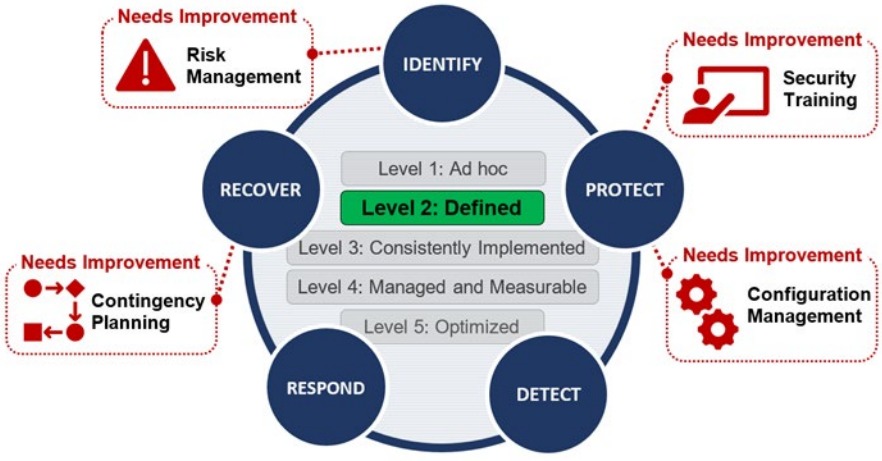
U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

U.S. Chemical Safety Board

CSB's Information Security Program Is Not Consistently Implemented; Improvements Are Needed to Address Four Weaknesses

Report No. 21-E-0071 **February 9, 2021**



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 CSB's information security program is not yet consistently implemented. Improvements are needed in risk management, configuration management, security training, and contingency planning. (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

U.S. Environmental Protection Agency
Office of Inspector General

21-E-0071
February 9, 2021

At a Glance

Why We Did This Evaluation

This evaluation was performed to assess the U.S. Chemical Safety and Hazard Investigation Board's compliance with performance measures outlined in the fiscal year 2020 inspector general reporting instructions for the Federal Information Security Modernization Act of 2014.

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

The *FY 2020 IG FISMA Reporting Metrics* outlines and provides potential ratings for security function areas to help federal agencies manage cybersecurity risks.

This report addresses the following:

- *Preserve the public trust by maintaining and improving organizational excellence.*

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

List of OIG reports.

CSB's Information Security Program Is Not Consistently Implemented; Improvements Are Needed to Address Four Weaknesses

What We Found

The CSB has not consistently implemented its information security program's policies, procedures, and strategies.

The SB & Company assessed the effectiveness of the CSB's information security program at "Level 2, Defined." A Level 2 designation means that the CSB's policies, procedures, and strategies are formalized and documented but not consistently implemented. While the CSB has policies, procedures, and strategies in place for information security, the SB & Company identified the following four weaknesses:

- The CSB did not have a governance structure to facilitate an organizationwide risk-management monitoring and reporting process.
- The CSB did not have a documented process that defines requirements for remediating flaws, including using a plan of actions and milestones to monitor the required remediation from initiation to resolution.
- The CSB did not have processes to provide privacy awareness training to all users and specialized training for individuals who support information security- or technology-related areas.
- The CSB discontinued information recovery testing and off-site backup storage during the coronavirus pandemic—that is, the SARS-CoV-2 virus and resultant COVID-19 disease. These issues were initially identified in OIG Report No. 21-E-0016, *CSB Discontinued Information Recovery Testing and Off-Site Backup Storage During the Coronavirus Pandemic,* issued November 18, 2020.

Appendix A contains the results of the FISMA assessment.

Recommendations and Planned Corrective Actions

The SB & Company made five recommendations to the CSB. The CSB agreed with the recommendations and provided acceptable corrective actions. Corrective action is pending for Recommendations 1 and 2 and completed for Recommendations 3, 4, and 5.

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

THE INSPECTOR GENERAL

February 9, 2021

Katherine A. Lemos, PhD
Chairperson and Chief Executive Officer
U.S. Chemical Safety and Hazard Investigation Board
1750 Pennsylvania Avenue NW, Suite 910
Washington, D.C. 20006

Dear Dr. Lemos:

This is a report on the U.S. Chemical Safety and Hazard Investigation Board's information security program. The report synopsizes the results of information technology security work performed by the SB & Company LLC under the direction of the U.S. Environmental Protection Agency's Office of Inspector General. The report also includes the SB & Company's completed fiscal year 2020 Federal Information Security Management Act reporting template, as prescribed by the Office of Management and Budget. The project number for this evaluation was OA&E-FY20-0034. 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 findings that describe the problems the SB & Company has identified and corrective actions the SB & Company recommends.

Your office provided acceptable corrective actions in response to the SB & Company's 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

Appendices

FY 2020 U.S. Chemical Safety and Hazard Investigation Board

Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics

Table of Contents

Appendices

Independent Accountants' Report

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) 2020 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 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, 2019 to September 30, 2020. 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, Background, Scope, and Methodology. Appendix A contains the FISMA Matrix 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 eight FISMA metric domains. Based on the results entered into CyberScope, we determined that CSB's overall information security program was "Defined" because a majority of the FY 2020 FISMA metrics were rated Defined (Level 2). We reported deficiencies impacting specific CyberScope questions in Identify (risk management), Protect (configuration management, and data protection and privacy), and Recover (contingency planning).

In our report, we have provided the Chief Information Officer (CIO) 5 findings and 5 recommendations that when addressed should strengthen CSB's information security program. The CSB CIO generally agreed with our conclusions and recommendations (see Management Response, page 36).

This independent evaluation did not constitute an engagement in accordance with Generally Accepted Government Auditing Standards. SBC 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.

This document reflects the final report and includes CSB Management responses. We met with the CSB management to discuss its response and modified the final report as needed. We consider the four recommendations resolved with corrective actions for two completed and two still pending. The CSB's complete response is in Appendix C.

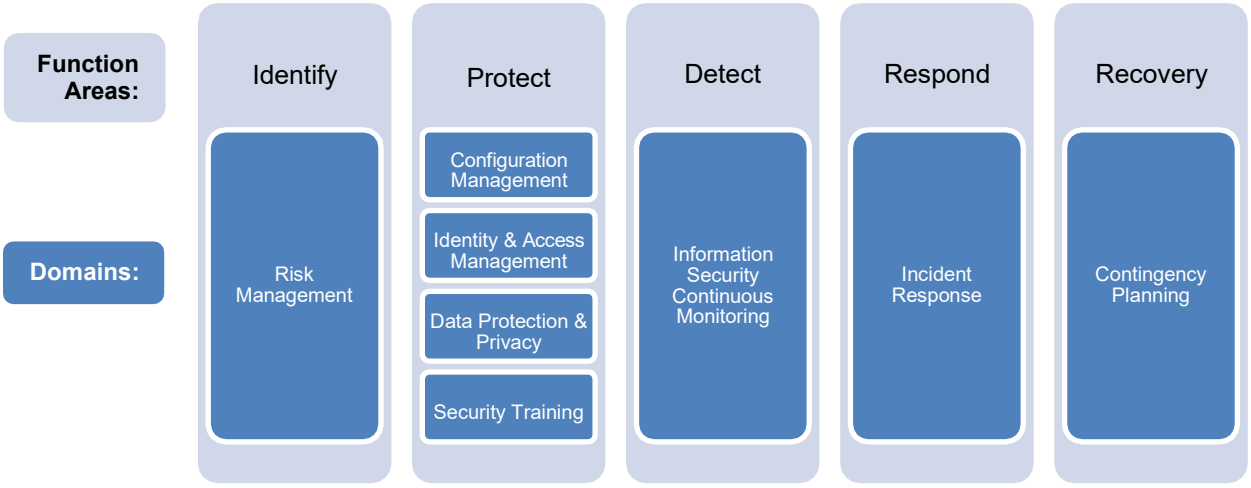
January 21, 2021

Background

Under 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 IG of each federal agency to use to assess the agency's information security program. The *FY 2020 IG FISMA Reporting Metrics*,[1] which can be found in Appendix A, identifies eight domains within the five security functions defined in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (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 2020 cybersecurity framework security function areas and domains



Source: OIG-created graphic based on *FY 2020 IG FISMA Reporting Metrics* information.

The effectiveness of an agency's information security program is based on a five-

[1] *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics,* Version 1.4, dated April 17, 2020. These metrics were developed as a collaborative effort between the Office of 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.

tiered maturity model spectrum (Table 1). An agency's IG is responsible for annually assessing the agency's rating along this spectrum by determining whether the agency possesses the required policies, procedures and strategies for each of the eight 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 2020 IG FISMA Reporting Metrics*.

Scope and Methodology

We conducted this evaluation from June to October 2020 in accordance with 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 1, *Ad-Hoc*, for each of the 67 questions for the eight domains in the *FY 2020 IG FISMA Reporting Metrics*. We conducted a risk assessment of the FY 2020 IG FISMA metrics to determine whether changes made to the underlying criteria of the FISMA metric questions significantly changed since the FY 2020 evaluation.

We also evaluated the new FY 2020 criteria to assess whether they significantly changed the CSB's responses to the overall metric questions since the FY 2019 audit. We assessed each new criterion as either:

- High Risk—The Office of Management and Budget introduced new reporting metrics, or the CSB made significant changes to its information security program since the FY 2019 audit for the identified metric question.

- Low Risk—The CSB made no significant changes to its information security program since the FY 2019 audit for the identified metric question.

We relied on the responses to the FY 2019 CSB FISMA metric questions to answer the FY 2020 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 closely with the CSB and briefed the agency on the audit results for each function area of the *FY 2020 IG FISMA Reporting Metrics*.

Appendix A provides the OIG response to each FISMA metric, as submitted to the Office of Management and Budget on October 7, 2020.

Prior Audit

During our testing of the CSB's FY 2020 FISMA compliance, SBC followed up on deficiencies identified in the FY 2019 FISMA evaluation, as documented in Report No. 20-P-0077 CSB's Information Security Program Is Defined, but Improvements Needed in Risk Management, Identity and Access Management, and Incident Response, dated February 12, 2020. The EPA OIG Office reported that the CSB lacked documented procedures and needed improvement in three domains: (1) Risk Management, (2) Identity and Access Management, and (3) Incident Response. Specifically, SBC found that the CSB did not:

1 Define and document risk management procedures for identifying, assessing, and managing information technology supply chain risk.

2 Define and implement processes for the use of Personal Identity Verification cards for logical access.

3 Define and document incident handling capabilities for the eradication of security incidents, as required by the National Institutes of Standards and Technology, Special Publication 800-53, Revision 4, Security Control: Incident Response.

The CSB completed corrective actions for the recommendations 2 and 3 listed above. See Appendix B for more details on the status of these corrective actions.

Results

The CSB's information security program 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-Function 1	Risk Management	Level 2, *Defined*
Protect -Function 2A	Configuration Management	Level 2, *Defined*
Protect-Function 2B	Identity and Access Management	Level 2, *Defined*
Protect-Function 2C	Data Protection and Privacy	Level 2, *Defined*
Protect-Function 2D	Security Training	Level 2, *Defined*
Detect-Function 3	Information Security Continuous Monitoring	Level 2, *Defined*
Respond-Function 4	Incident Response	Level 2, *Defined*
Recover-Function 5	Contingency Planning	Level 2, *Defined*

Source: *FY 2020 IG FISMA Reporting Metrics*.

However, in FY 2020, the CSB continued to need improvements for specific questions in the "Risk Management," "Configuration Management," "Data Protection and Privacy," "Security Training," and "Contingency Planning" domains, as shown in Table 3.

Table 3: CSB domains that require further improvement

Function area	Domain	FISMA questions that need improvement
Identify	Risk Management	The CSB has not performed Risk Management Assessment processes that comply with NIST 800-37 within the last twelve months. In addition, a governance structure has not been put in place to facilitate an organization-wide Risk Management monitoring and reporting process. *See Appendix A, FISMA Questions 5 and 12.*
Identify	Risk Management	The CSB does not have a documented process that defines requirements for designating the use of POAMs (Plan of Action and Milestones) to monitor required flaw remediation to resolution. *See Appendix A, FISMA Question 8.*
Protect	Configuration Management	The CSB does not have a documented process that defines requirements for addressing flaw remediation including how POAMS should be used to monitor required remediation to resolution. *See Appendix A, FISMA Question 19.*
Protect	Data Protection and Privacy	The CSB Security Training processes are not in place to ensure that privacy awareness training is provided to all users. *See Appendix A, FISMA Question 37.*
Protect	Security Training	The CSB has not defined and implemented Information Security awareness training and specialized training for individuals that have a role supporting Information Security or Technology-related areas. The CSB has not formally documented an Information Security and awareness strategy that leverages their organizational skills assessment and factors the training program priorities, funding, the goals of the program and targeted audiences. *See Appendix A, FISMA Questions 41, 42, and 44.*
Recover	Contingency Planning	The CSB has not performed disaster recovery testing in the last twelve months. In addition, the CSB has not maintained copies of backup media at an offsite location to ensure that these resources are available to recover critical systems. *See Appendix A, FISMA Question 64.*

Source: SBC Recap

Conclusion

The CSB would greatly improve and strengthen its cybersecurity program by fully performing a risk assessment on an annual basis. Annual risk assessments would allow the agency to identify emerging risks, to guard against attacks on its network and keep critical resources available for end-users. Likewise, the use of POAM's in addressing flaw remediation to monitor required remediation to resolution would greatly enhance the CSB's cybersecurity program by providing the agency a consistent approach to flaw remediation.

The CSB would improve its cybersecurity program by developing and implementing processes to ensure that privacy awareness training is provided to all users and Information Security awareness training and specialized training is provided for individuals that have a role supporting Information Security or technology related areas. Additionally, the CSB should formally document an Information Security and awareness strategy that leverages their organizational skills assessment and factors the training program priorities, funding, the goals of the program and targeted audiences.

The CSB would strengthen its cybersecurity program by scheduling and performing disaster recovery testing on an annual basis. In the event of an actual disaster, annual disaster recovery testing would allow the agency to respond more efficiently and predictably in restoring agency operations. Likewise, the CSB would ensure that they will be able to recover critical systems in the advent of a disaster at their primary location by maintaining copies of backup media at an offsite location.

Recommendations

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

1. 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.
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 monitoring on the timeliness of applying patch updates.
3. Implement a process to ensure that privacy awareness training is provided to all individuals, including role-based training where needed.

4. Implement Information Security awareness and specialized security training policies and procedures to provide exposure to areas specific to individuals that have a role supporting 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.
5. Perform disaster recovery testing on an annual basis. In addition, evaluate alternate methods to store backup media offsite.

CSB Response and Procedures Performed

The CSB agreed with two of the four draft recommendations and provided acceptable planned corrective actions and milestone dates. The CSB stated it would perform a risk assessment by December 31, 2020. We consider this recommendation resolved with corrective action pending. The CSB stated that it will develop a more formal process for documenting risk acceptances and timelines for patch updates by January 31, 2021. The CSB stated that the privacy awareness training module was issued to all employees on October 21, 2020 and submitted support. We consider this recommendation resolved.

In addition, the CSB resumed maintaining offsite back-ups and performed disaster recovery testing as part of moving files from the Western Regional Office (WRO) back to the Washington headquarters. Documentation has been submitted and this item also concluded as closed.

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	1, 4	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.	R		4/30/2021	
2	3, 6	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 monitoring on the timeliness of applying patch updates.	R		1/31/2021	
3	9	Implement a process to ensure that privacy awareness training is provided to all individuals, including role-based training where needed.	C		11/30/2020	
4	9-10	Implement Information Security awareness and specialized security training policies and procedures to provide exposure to areas specific to individuals that have a role supporting 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.	C		12/31/2020	
5	13	Perform disaster recovery testing on an annual basis. In addition, evaluate alternate methods to store backup media offsite.	C		12/31/2020	

[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

2020

Annual FISMA Report

Chemical Safety Board

Function 1: 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. 4: CA-3, PM-5, and CM-8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2020 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).

Defined (Level 2)

Comments: CCSB has a defined process to maintain comprehensive inventory of its information systems.

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. 4: CA-7 and CM-8; NIST SP 800-137; NISTIR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2020 CIO FISMA Metrics: 1.2

Defined (Level 2)

Comments: CSB has a defined process to maintain comprehensive inventory of its information systems.

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 (NIST SP 800-53 Rev. 4: CA-7, CM-8, and CM-10; NIST SP 800-137; NISTIR 8011; FEA Framework, v2; FY 2020 CIO FISMA Metrics: 1.2.5, 1.3.3, 3.10; CSF: ID.AM-2)?

Defined (Level 2)

Comments: CSB has a defined process to maintain comprehensive inventory of its information systems.

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 2020 CIO FISMA Metrics: 1.1; OMB M-19-03)?

Defined (Level 2)

Comments: Verified that CSB has categorized and communicated the importance and priority of information systems in enabling its missions and business functions, including for high value assets.

Function 1: Identify - Risk Management

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy, including for supply chain risk management. This includes the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST SP 800-39; NIST SP 800-53 Rev. 4: PM-8, PM-9; CSF: ID RM-1 - ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; NIST SP 800-37 (Rev. 2); NIST SP 800-161: Appendix E; CSF: ID.SC-1 - 2; SECURE Technology Act: s. 1326, Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019)?

Ad Hoc (Level 1)

Comments: Based on our follow up discussion with CSB information technology management, while a risk assessment process is in place, a risk assessment has not been performed in last 12 months due to pandemic.

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); 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: Verified that CSB has defined an information security architecture and described how that architecture is integrated into and supports the organization’s enterprise architecture.

7 To what degree have roles and responsibilities of internal and external stakeholders involved in risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; OMB A-123; CFO Council ERM Playbook; NIST SP 800-37 (Rev. 2); OMB M-19-03)?

Defined (Level 2)

Comments: Verified that roles and responsibilities of stakeholders have been defined and communicated across CSB.

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); OMB M-19-03, CSF v1.1, ID.RA-6)?

Ad Hoc (Level 1)

Comments: Based on our follow up discussion with CSB information technology management, based on the size of the CSB organization, tracking is currently an informal manual process. Currently, CSB has implemented an IT POA&M tracking sheet; however, there is not a documented procedure in place that defines how the tracking sheet will be used to mitigate any security weakness identified.

Function 1: Identify - Risk Management

9 To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing (i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework (ii) internal and external asset vulnerabilities, including through vulnerability scanning, (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and (iv) security controls to mitigate system-level risks (NIST SP 800-39; NIST SP 800-53 REV. 4: PL-2 and RA-1; NIST SP 800-30; CSF: Section 4.0; NIST SP 800-37 (Rev. 2))?

Defined (Level 2)

Comments: CSB uses the GFI Languard software to perform vulnerability assessments on the Internal network. The software has the ability to rank risk exposures identified as High, Medium and Low.

10 To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; SECURE Technology Act: s. 1326)?

Defined (Level 2)

Comments: Verified that CSB has defined how information about risks are communicated in a timely manner to all necessary internal and external stakeholders.

11 To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (NIST SP 800-53 REV. 4: SA-4; NIST SP 800-152; NIST SP 800-37 Rev. 2; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4).

Defined (Level 2)

Comments: The CSB has defined a process that includes information security and other business areas as appropriate for ensuring that contracts and other agreements for third party systems and services include appropriate clauses to monitor the risks related to such systems and services.

12 To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?

Ad Hoc (Level 1)

Comments: Based on our discussion with CSB information technology management, due to the size and resources of the organization, processes related to governance and process management are handled through manual informal processes.

Function 1: Identify - Risk Management

13.1 Please provide the assessed maturity level for the agency's Identify - Risk Management function.

Defined (Level 2)

Comments: Defined - Based on the maturity level of the individual areas within Risk Management, the overall maturity level is concluded as "Defined."

13.2 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?

Defined - Based on the maturity level of the individual areas within Risk Management, the overall maturity level is concluded as "Defined."

Calculated Maturity Level - Defined (Level 2)

Function 2A: Protect - Configuration Management

14 To what degree 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: Verified by review of the CSB's Configuration Management policy and identified that roles and responsibilities at the organizational and information system levels for stakeholders involved in information system configuration management have been fully defined and communicated across the organization.

15 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: Verified by review of the CSB's Configuration Management policy and identified that the policy does define roles and responsibilities for configuration management. The policy also defines processes included in change management and system development life cycle.

16 To what degree have information system configuration management policies and procedures been defined and implemented across the organization ? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: 2.2.1)

Defined (Level 2)

Comments: CSB has developed, documented, and disseminated comprehensive policies and procedures for managing the configurations of its information systems.

Function 2A: Protect - Configuration Management

17 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 2020 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?

Defined (Level 2)

Comments: Verified by review of the CSB's Configuration Management policy and identified that the CSB has developed, documented, and disseminated its baseline configuration and component inventory policies and procedures.

18 To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53 REV. 4: CM-6, CM-7, RA-5, and SI-2; NIST SP 800-70, Rev. 4, FY 2020 CIO FISMA Metrics: 2.1, 2.2, 2.14, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?

Defined (Level 2)

Comments: Verified by review of the CSB's Configuration Management policy and the inventory baseline file and identified that the CSB has developed, documented, and disseminated its policies and procedures for configuration settings/common secure configurations.

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; SANS/CIS Top 20, Control 4.5; FY 2020 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directive (BOD) 15-01; DHS BOD 18-02)?

Ad Hoc (Level 1)

Comments: Verified by review of the CSB's IT POA&M tracking sheet that the CSB is using a tracking sheet to log patches and security updates. However, the CSB has not developed, documented, and disseminated its policies and procedures for flaw remediation, including mobile devices.

20 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: CSB has entered relationships with various agencies to maintain trust relationship includes Homeland of Security to leverage the use of Einstein software to protect information systems.

Function 2A: Protect - Configuration Management

21 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: Verified by review of the CSB's Configuration Management policy and identified that CSB has developed, documented, and disseminated its policies and procedures for managing configuration change control. The policies and procedures address the review and approval/disapproval of proposed changes, retaining records of implemented changes, and coordination and oversight of changes by the CSB.

22 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?

Based on the maturity level of the individual areas within Configuration Management, the overall section is concluded as "Defined."

Calculated Maturity Level - Defined (Level 2)

Function 2B: Protect - Identity and Access Management

23 To what degree 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; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Defined (Level 2)

Comments: Based on the review of IT security program, roles and responsibilities for identity, credential, and access management have been defined.

24 To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?

Defined (Level 2)

Comments: Verified that the CSB organization has defined its ICAM strategy by identification of how authentication requirements are in place for all of its' systems. Verified that the CSB network requires authentication to log on.

Function 2B: Protect - Identity and Access Management

25 To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 26 through 31) (NIST SP 800-53 REV. 4: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

Defined (Level 2)

Comments: Verified that the CSB organization has defined its ICAM policies in place.

26 To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate 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)?

Defined (Level 2)

Comments: 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.

27 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 PS6)?

Defined (Level 2)

Comments: CSB has in place policies and process for access, nondisclosure and acceptable use agreements for both privileged and non-privileged users that access its systems.

28 To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.4 and 2.7; CSF: PR.AC-1 and 6; and Cybersecurity Sprint)?

Defined (Level 2)

Comments: CSB has mechanisms in place to require strong authentication processes in place. Efforts should continue to complete the roll-out of multi-factor authentication.

29 To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01; and Cybersecurity Sprint)?

Defined (Level 2)

Comments: CSB has mechanisms in place to require strong authentication processes in place. Efforts should continue to complete the roll-out of multi-factor authentication.

Function 2B: Protect - Identity and Access Management

30 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 (FY 2019 CIO FISMA Metrics: 2.3 and 2.5; NIST SP 800-53 REV. 4: AC-1, AC-2 (2), and AC-17; CSIP; DHS ED 19- 01; CSF: PR.AC-4).

Defined (Level 2)

Comments: CSB has mechanisms in place to require strong authentication processes in place. Efforts should continue to complete the roll-out of multi-factor authentication.

31 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-17 and SI-4; CSF: PR.AC-3; and FY 2019 CIO FISMA Metrics: 2.10)?.

Defined (Level 2)

Comments: CSB uses VPN connection to provide remote access. CSB has defined its configuration/connection requirements for remote access connections, including use of cryptographic modules, system time-outs, and how it monitors and controls remote access sessions. CSB should continue efforts to mature these processes.

32 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 for the individual areas, the overall maturity level concluded for Identity and Access Management is "Defined."

Calculated Maturity Level - Defined (Level 2)

Function 2C: Protect - Data Protection and Privacy

33 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); OMB M-18- 02; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J)?

Defined (Level 2)

Comments: CSB has developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems.

Function 2B: Protect - Identity and Access Management

34 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? (NIST SP 800-53 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2019 CIO FISMA Metrics: 2.8; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)?

- ·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: CSB has developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems.

35 To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses ? (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2019 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

Defined (Level 2)

Comments: CSB has developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems.

36 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 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17- 25)?

Defined (Level 2)

Comments: CSB has documented and implemented a Data Breach Response Plan.

37 To what degree 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)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)

Ad Hoc (Level 1)

Comments: CSB should ensure that all individuals receive basic privacy awareness training and individuals having responsibilities for PII or activities involving PII receive role-based privacy training at least annually.

Function 2B: Protect - Identity and Access Management

38 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 conclusion for the individual questions in this section, the overall maturity level for Data Protection and Privacy is concluded as "Defined".

Calculated Maturity Level - Defined (Level 2)

Function 2D: Protect - Security Training

39 To what degree 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: Verified that Roles and responsibilities have been defined and communicated across CSB and resource requirements have been established.

40 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 (NIST SP 800-53 REV. 4: AT-2 and AT-3; 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/SANS Top 20: 17.1)?

Defined (Level 2)

Comments: Verified that CSB has defined its processes for conducting an assessment of the knowledge, skills, and abilities of its workforce to determine its awareness and specialized training needs and periodically updating its assessment to account for a changing risk environment.

41 To what extent 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).

Defined (Level 2)

Comments: CSB has implemented and continues to perform organization-wide security awareness and training plan.

Function 2D: Protect - Security Training

42 To what degree have security awareness and specialized security training policies and procedures been defined and implemented ? (Note: the maturity level should take into consideration the maturity of questions 43 and 44 below) (NIST SP 800-53 REV. 4: AT-1 through AT-4; and NIST SP 800-50).

Ad Hoc (Level 1)

Comments: CSB should ensure that its' policies and procedures for security awareness and specialized security training are performed.

43 To what degree 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 2019 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).

Defined (Level 2)

Comments: CSB has policies and procedures in place to define security training requirements.

44 To what degree 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 2019 CIO FISMA Metrics: 2.15)?

Ad Hoc (Level 1)

Comments: CSB should ensure that individuals with significant security responsibilities are provided specialized security training.

45.1 Please provide the assessed maturity level for the agency's Protect Function.

Defined (Level 2)

Comments: The individual questions were concluded across both the Ad hoc (2) and Defined maturity levels. Because the processes are documented, the overall maturity level will be concluded as "Defined".

45.2 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?

The individuals questions were concluded across both the Ad hoc (2) and Defined maturity levels. Because the processes are documented, the overall maturity level will be concluded as "Defined".

Calculated Maturity Level - Defined (Level 2)

Function 3: Detect – Information Security Continuous Monitoring (ISCM)

46 To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organizationwide approach to ISCM (NIST SP 800-37 (Rev. 2); NIST SP 800-137: Sections 3.1 and 3.6)?.

Defined (Level 2)

Comments: CSB has put in place an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements.

47 To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collection of security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53 REV. 4: CA-7, NISTIR 8011) (Note: The overall maturity level should take into consideration the maturity of question 49)?.

Defined (Level 2)

Comments: CSB has put in place an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements.

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; and FY 2019 CIO FISMA Metrics)?.

Defined (Level 2)

Comments: CSB has put in place an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements including the roles and responsibilities of stakeholders.

49 How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800- 137: Section 2.2; NIST SP 800- 53 REV. 4: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2); NISTIR 8011; OMB M-14-03; OMB M-19-03)

Defined (Level 2)

Comments: CSB has documented processes for performing ongoing assessments , granting system authorizations, and monitoring security controls.

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 3)

Comments: The CSB's process for collecting and analyzing ISCM performance measures and reporting findings is systemic and allows through the use of tools like Malware Bytes and MTIPS 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 Function.

Defined (Level 2)

Comments: Based on the maturity level for the individual questions, the overall maturity level for Detect 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 for the individual questions, the overall maturity level is concluded as "Defined".

Calculated Maturity Level - Defined (Level 2)

Function 4: Respond - Incident Response

52 To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53 REV. 4: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800- 184; OMB M-17-25; OMB M- 17-09; FY 2018 CIO FISMA Metrics: 4.2; CSF: RS.RP-1; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58).

Defined (Level 2)

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

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; OMB M-18-02; OMB M-16-04; FY 2019 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

Defined (Level 2)

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

54 How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-18-02; CSF: DE.AE-1, PR.DS-6, RS.AN-4, and PR.DS- 8; and US-CERT Incident Response Guidelines)

Defined (Level 2)

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

55 How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)

Defined (Level 2)

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

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-18-02; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 4; DHS Cyber Incident Reporting Unified Message)

Defined (Level 2)

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

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-18-02; PPD-41).

Defined (Level 2)

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

58 To what degree 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: CSB has defined and communicated the structures of its incident response teams, roles and responsibilities of incident response stakeholders, and associated levels of authority and dependencies.

59.1 Please provide the assessed maturity level for the agency's Respond - Incident Response function.

Defined (Level 2)

Comments: Defined- Based on the maturity level for the individual questions, the overall maturity level is “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 for the individual questions in this section, the overall maturity level is concluded as “Defined."

Calculated Maturity Level - Defined (Level 2)

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 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

Consistently Implemented (Level 3)

Comments: Verified by review of the CSB Information System Contingency Plan that CSB has defined Individuals ‘roles and responsibilities of stakeholders involved in information systems contingency planning across the organization.

61 To what extent has the organization defined and implemented its information system contingency planning program through policies , procedures, and strategies, as appropriate (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 62-66) (NIST SP 800-34; NIST SP 800- 161; CSF: ID.BE-5, PR.IP-9, and ID.SC-5).

Defined (Level 2)

Comments: Verified by review of the CSB Information System Contingency Plan that the organization has defined and implemented its information system contingency planning program through policies, procedures, and strategies, to prioritize the recovery of business critical Information Systems.

62 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17- 09; FY 2019 CIO FISMA Metrics: 5.1; CSF:ID.RA-4)?

Defined (Level 2)

Comments: Verified by review of the CSB Information System Contingency Plan that the organization has defined and implemented its information system contingency planning program through policies, procedures, and strategies, to prioritize the recovery of business critical Information Systems.

63 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 2019 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

Defined (Level 2)

Comments: Verified by review of the CSB Information System Contingency Plan that the organization has defined and implemented its information system contingency planning program through policies, procedures, and strategies, to prioritize the recovery of business critical Information Systems.

64 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2019 CIO FISMA Metrics: 5.1; CSF: ID.SC-5 and CSF: PR.IP-10)?

Ad Hoc (Level 1)

Comments: As a result of COV-19, disaster recovery testing has not been performed in the last twelve months.

65 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; NIST CSF: PR.IP-4; FY 2019 CIO FISMA Metrics: 5.1.1; and NARA guidance on information systems security records)?

Defined (Level 2)

Comments: Processes are in place to perform back-up and storage; however, as a result of COV-19 protocols back-up media was not being rotated off-site.

66 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: Processes are in place to perform back-up and storage as well as perform disaster recovery testing are documented; however, as a result of COV-19 protocols back-up media was not being rotated off-site and disaster recovery testing had not been performed in the last twelve months.

67.1 Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.

Defined (Level 2)

Comments: Defined – Based on the maturity level concluded for the individual areas, the overall maturity level is concluded as “Defined.”

67.2 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 for the individual questions, the overall maturity level is concluded as "Defined."

Calculated Maturity Level - Defined (Level 2)

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.

·Do not include the names of specific independent auditors, these entities should be referred to as "independent assessor" or "independent auditor"

·The assessment of effectiveness should not include a list of ratings by NIST CSF Function-level, as these will already be included in the performance summary

This matrix was completed by an independent assessor that performed the work as directed under contract with the EPA's Office of Inspector General.

The U.S. Chemical Safety and Hazard Board's Information Security Program continues to mature. During the FISMA Assessment, concerns were identified related to Risk Management, Flaw Remediation, Training, Disaster Recovery Testing and Maintaining Back-ups at an Alternate Location. The concerns related to Disaster Recovery Testing and maintaining back-ups at an alternate location are areas where the design of procedures were adequate; however, the related operating processes had been discontinued as a direct result of COV-19 protocols. Recommendations have been made to enhance the control environment in areas where concerns were identified. The overall design of the Information Security Program has been concluded as effective, and procedures in place are adequate and situate this agency for continued growth in the maturity of these processes.

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	3
Defined	9
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2) Not Effective	

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	1
Defined	7
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2) Not Effective	

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	9
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2) Not Effective	

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	1
Defined	4
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2) Not Effective	

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	2
Defined	4
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2) Not Effective	

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	4
Consistently Implemented	1
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2) Not Effective	

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	7
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2) Not Effective	

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	1
Defined	5
Consistently Implemented	1
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2) Not Effective	

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Defined (Level 2)	Defined (Level 2)	Defined - Based on the maturity level of the individual areas within Risk Management, the overall maturity level is concluded as “Defined.”
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Defined (Level 2)	Defined (Level 2)	The individuals questions were concluded across both the Ad hoc (2) and Defined maturity levels. Because the processes are documented, the overall maturity level will be concluded as “Defined”.
Function 3: Detect - ISCM	Defined (Level 2)	Defined (Level 2)	Based on the maturity level for the individual questions, the overall maturity level for Detect is concluded as “Defined.”
Function 4: Respond - Incident Response	Defined (Level 2)	Defined (Level 2)	Defined- Based on the maturity level for the individual questions, the overall maturity level is “Defined”.
Function 5: Recover - Contingency Planning	Defined (Level 2)	Defined (Level 2)	Defined – Based on the maturity level concluded for the individual areas, the overall maturity level is concluded as “Defined.”
Overall	Not Effective	Effective	

Appendix B

Status of CSB Corrective Actions for Prior FISMA Audit Recommendations

The table below describes the recommendations from previous FISMA audits that remained unimplemented as of February 2020, when we published our last FISMA audit report.

OIG Report	Recommendation		Corrective action	OIG analysis of corrective action status
No. 20-P-0077, *CSB's Information Security Program Is Defined, but Improvements Needed in Risk Management, Identity and Access Management, and Incident Response,* dated February 12, 2020	1	Define and document risk management procedures for identifying, assessing and managing information technology supply chain risk.	The CSB has documented a supply chain risk management policy to indicate the procedures to be put in place to manage supply chain risk exposures.	**Completed 7/15/20**
	2	Define and document incident handling capabilities for the eradication of security incidents, as required by the National Institute of Standards and Technology, Special Publication 800-53, Revision 4, *Security Control: Incident Response-4*.	The CSB has documented an incident response policy, which addresses the phases of incident response as identified by the National Institute of Standards and Technology, Special Publication 800-53 Revision 4.	**Completed 7/20/20**
No. 19-P-0147, *CSB Still Needs to Improve Its "Incident Response" and "Identity and Access Management" Information Security Functions,* dated May 9, 2019*	1	Implement use of Homeland Security Presidential Directive-12, regarding Personal Identity Verification card technology for physical and logical access, as required. If unable to implement this card technology, obtain a waiver from the Office of Management and Budget not to operate as required by the National Institute of Standards and Technology.	MYKastle card access software has been put in place to manage and define permissions to physically access sensitive areas. The access cards are now operated 24x7 to obtain access through the front door, suite, and data center area. Multifactor authentication has been put in place but is limited to information technology. There is a test group outside of information technology that is using multifactor authentication. The time frame and complete roll-out of multifactor authentication to all employees still remains to be determined.	**Partially implemented/ In process** **Planned completion date: 4/30/21**

*During the evaluation, it was determined that the corrective actions for Recommendations 2, 3, 4, and 5 have been implemented.

CSB Response to Draft Report

U.S. Chemical Safety and Hazard Investigation Board

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

Honorable Katherine A. Lemos
Chairman and CEO

January 15, 2021

Mr. Albert Schmidt
c/o EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, DC 20460

Dear Mr. Schmidt:

Thank you for the opportunity to review the Office of Inspector General's (OIG's) FY2020 Federal Information Security Modernization Act of 2014 (FISMA) draft audit report.

The CSB has reviewed the report and offers the following comments and observations with respect to the weaknesses identified.

WEAKNESS: The CSB does not have a governance structure to facilitate an organization-wide risk-management monitoring and reporting process.

The CSB agrees with this finding and will produce a governance structure with a risk management plan that addresses a number of concepts. By April 30, we will submit a governance structure document that will address the following topics:

- Standard operations and resource responsibilities
- Response plans (normal, degraded, off-line)
- Risk management framework
- Monitoring and testing
- POAM process

When possible, we will submit individual pieces of the document as they are created.

WEAKNESS: The CSB does not have a documented process that defines requirements for addressing flaw remediation, including how a plan of actions and milestones should be used to monitor required remediation to resolution.

The CSB agrees with this finding and will revise its Plan of Action and Milestones (**POA&M**) form to incorporate timelines and monitoring requirements. We expect the form to be completed by January 31, 2021.

U.S. Chemical Safety and Hazard Investigation Board

WEAKNESS: The CSB did not have processes to provide privacy awareness training to all users and specialized training for individuals who support information security- or technology-related areas.

The CSB issued a privacy awareness training module to all employees on October 21, 2020. All employees have completed the training and submitted signed evaluation forms as of November 30, 2020. We have submitted documentation to the EPA OIG, and we consider this item CLOSED.

WEAKNESS: The CSB discontinued information recovery testing and off-site back-up storage during the coronavirus pandemic. These issues were identified in a previous OIG Evaluation (Report No. 21-E-0016), and the CSB plans to complete corrective actions to resolve the deficiency by December 31, 2020.

The CSB has renewed its contract with the vendor and resumed off-site backup storage. Documentation has been provided to the EPA OIG. In late November and again early December 2020, the CSB performed a real-time disaster recovery exercise in the process of moving essential services and files from its Western Regional Office (WRO) back to its Washington headquarters as part of the shutdown of the WRO office. We have submitted documentation on the successful disaster process to the EPA OIG, and we consider this item CLOSED.

We will update you on our progress as we work to close the remaining recommendations. If you have any questions, please contact our Chief Information Officer, Mr. Charlie Bryant, at (202) 261-7666.

Sincerely,

Dr. Katherine Andrea Lemos

Digitally signed by Dr. Katherine Andrea Lemos
Date: 2021.01.14 15:16:30 -05'00'

Dr. Katherine A. Lemos
Chairman and CEO

Appendix D

Distribution

Chairperson and Chief Executive Officer, U.S. Chemical Safety and Hazard Investigation Board
Board Members, U.S. Chemical Safety and Hazard Investigation Board
Chief Information Officer, U.S. Chemical Safety and Hazard Investigation Board
Deputy Chief Information Officer, U.S. Chemical Safety and Hazard Investigation Board
General Counsel, U.S. Chemical Safety and Hazard Investigation Board
Director of Administration and Audit Liaison, U.S. Chemical Safety and Hazard Investigation Board