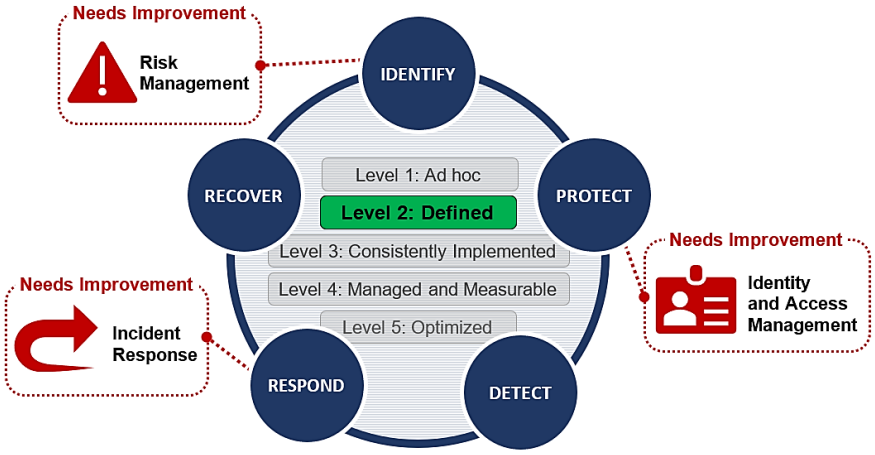
U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

U.S. Chemical Safety Board

CSB's Information Security Program Is Defined, but Improvements Needed in Risk Management, Identity and Access Management, and Incident Response

Report No. 20-P-0077 **February 12, 2020**



Report Contributors:

Rudolph M. Brevard
LaVonda Harris-Claggett
Iantha Maness
Christina Nelson
Jeremy Sigel
Sabrena Stewart

Abbreviations

CSB	U.S. Chemical Safety and Hazard Investigation Board
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG	Inspector General
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
U.S.C.	United States Code

Cover Image: OIG assessment of the CSB's FISMA function areas and domains. (EPA OIG graphic)

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

20-P-0077
February 12, 2020

At a Glance

CSB's Information Security Program Is Defined, but Improvements Needed in Risk Management, Identity and Access Management, and Incident Response

Why We Did This Project

We performed this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) compliance with performance measures outlined in the fiscal year (FY) 2019 Inspector General (IG) reporting instructions for the Federal Information Security Modernization Act of 2014 (FISMA).

The *FY 2019 IG FISMA Reporting Metrics* outlines five security function areas and eight corresponding domains to help federal agencies manage cybersecurity risks. The document also outlines five maturity levels by which IGs should rate agency information security programs:

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

This report addresses the following CSB goal:

- *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.

What We Found

The CSB lacks documented procedures to address information technology risks and threats from cybersecurity incidents.

We assessed the maturity 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. To determine the CSB's maturity level, we reviewed the five security function areas outlined in the *FY 2019 IG FISMA Reporting Metrics:* Identify, Protect, Detect, Respond and Recovery. We also reviewed the eight corresponding domains: Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning. While the CSB has policies, procedures and strategies for many of these function areas and domains, improvements are still needed in:

- **Risk Management**—The CSB neither identified nor defined its procedures for identifying, assessing or managing supply chain risks for the agency's information systems.

- **Identity and Access Management**—The CSB lacks processes to allow users to access its systems with Personal Identity Verification cards. This issue was identified in a previous Office of Inspector General audit (Report No. 19-P-0147), and the CSB plans to complete corrective actions to resolve the deficiency by March 31, 2020.

- **Incident Response**—The CSB did not define incident handling processes specific to eradication in its incident response procedures.

Appendix A contains the results of our FISMA assessment.

Recommendations and Planned Agency Corrective Actions

We recommend that the CSB (1) define and document risk management procedures for identifying, assessing and managing supply chain risk and (2) define and document incident handling capabilities for the eradication of security incidents.

The CSB agreed with our recommendations and provided or completed acceptable corrective actions. Corrective action is pending for Recommendation 1 and complete for Recommendation 2.

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

THE INSPECTOR GENERAL

February 12, 2020

Kristen Kulinowski, Ph.D.
Interim Executive Authority and Member
U.S. Chemical Safety and Hazard Investigation Board
1750 Pennsylvania Avenue NW, Suite 910
Washington, D.C. 20006

Dear Dr. Kulinowski:

This is the U.S. Environmental Protection Agency's Office of Inspector General (OIG) report on the audit of the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) compliance with the Federal Information Security Modernization Act (FISMA) of 2014. This report represents the opinion of the OIG and does not necessarily represent the final CSB position. The final determination on matters in this report will be made by CSB managers in accordance with established audit resolution procedures.

Your office provided or completed acceptable corrective actions in response to OIG recommendations. Corrective action is pending for Recommendation 1 and complete for Recommendation 2. No final response to this report is required. However, if you submit a response, 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

Sean W. O'Donnell

Table of Contents

Appendices

Purpose

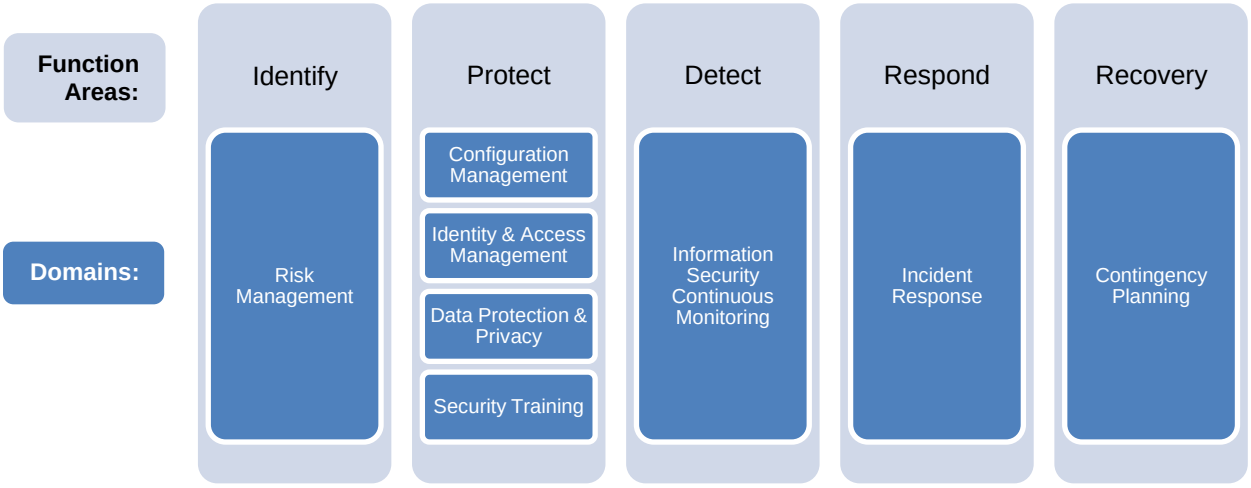
The Office of Inspector General (OIG) performed this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) compliance with the fiscal year (FY) 2019 Inspector General (IG) reporting metrics for the Federal Information Security Modernization Act of 2014 (FISMA).

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.[1]

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 2019 IG FISMA Reporting Metrics*,[2] 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).[3] This cybersecurity framework provides agencies with a common structure for identifying and managing cybersecurity risks to critical infrastructure across the enterprise.

Figure 1: FY 2019 cybersecurity framework security function areas and domains



Source: OIG-created graphic based on *FY 2019 IG FISMA Reporting Metrics* information.

[1] 44 U.S.C. § 3554(a)(1)(A).
[2] *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.3, dated April 9, 2019. 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 and Efficiency, in consultation with the Federal Chief Information Officer Council.
[3] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, was issued February 19, 2013, and directed NIST to develop a voluntary framework based on existing standards, guidelines and practices to reduce cyber risks to critical infrastructure.

The effectiveness of an agency's information security program is based on a five-tiered maturity model spectrum (Table 1). An agency's IG is responsible for annually assessing the agency's rating along this spectrum by determining whether the agency possesses the required policies, procedures and strategies for each of the 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 2019 IG FISMA Reporting Metrics*.

Responsible Offices

The CSB is an independent federal agency that is responsible for investigating industrial chemical accidents at fixed industrial facilities to determine the conditions and circumstances that led to the accidents, so that similar events might be prevented. As the agency head, the CSB's Chief Executive Officer is responsible for agency administration.[4] The CSB's Chief Information Officer, who reports to the Chief Executive Officer, supervises the administration of the information technology security program and oversees the CSB's compliance with FISMA requirements. The Chief Information Officer also reports to the agency head regarding the progress of remedial actions on the agency's information security program.

The CSB investigated an explosion and fire at the AB Specialty Silicones facility in Waukegan, Illinois. (CSB photo)

[4] The current title for the "Chief Executive Officer" role is "Interim Executive Authority and Member."

Scope and Methodology

We conducted this audit from June to November 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objective.

During our audit, we assessed whether the CSB exceeded Maturity Level 1, *Ad Hoc*, for each of the 67 questions for the eight domains in the *FY 2019 IG FISMA Reporting Metrics.* We conducted a risk assessment of the FY 2019 IG FISMA metrics to determine whether changes made to the underlying criteria of the FISMA metric questions significantly changed since the FY 2018 audit.

We also evaluated the new FY 2019 criteria to assess whether they significantly changed the CSB's responses to the overall metric questions since the FY 2018 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 2018 audit for the identified metric question.

- Low Risk—The CSB made no significant changes to its information security program since the FY 2018 audit for the identified metric question.

We relied on our responses to the FY 2018 CSB FISMA metric questions to answer the FY 2019 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 2019 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 18, 2019.

Prior Audit

During our testing of the CSB's FY 2019 FISMA compliance, we followed up on deficiencies identified in the FY 2018 FISMA audit, as documented in Report No. 19-P-0147, *CSB Still Needs to Improve Its "Incident Response" and "Identity and Access Management" Information Security Functions*, dated May 9, 2019. We reported that the CSB lacked documented procedures and needed improvement in three domains: (1) Identity and Access Management, (2) Data Protection and Privacy, and (3) Incident Response. Specifically, we found that the CSB did not:

- Define or implement processes regarding Personal Identity Verification cards for physical and logical access.
- Define policies or procedures for data exfiltration and enhanced network defenses.
- Identify or define its incident handling policies and procedures to address containment, eradication and recovery of systems.
- Document or formalize its rationale for not having an automated system for the detection of potential incidents.
- Document procedures to generate alerts based on log data analysis and record pertinent data of suspicious activity to respond to cybersecurity events.

The CSB completed corrective actions for the last four recommendations in the list 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	Risk Management	Level 2, *Defined*
Protect	Configuration Management	Level 2, *Defined*
Protect	Identity and Access Management	Level 2, *Defined*
Protect	Data Protection and Privacy	Level 2, *Defined*
Protect	Security Training	Level 2, *Defined*
Detect	Information Security Continuous Monitoring	Level 2, *Defined*
Respond	Incident Response	Level 2, *Defined*
Recover	Contingency Planning	Level 2, *Defined*

Source: *FY 2019 IG FISMA Reporting Metrics*.

However, in FY 2019, the CSB continued to need improvements for specific questions in the "Risk Management," "Identity and Access Management," and "Incident Response" 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 neither identified nor defined its risk management procedures for identifying, assessing or managing supply chain risk.* *See Appendix A, FISMA Questions 5 and 6.*
Protect	Identity and Access Management	The CSB did not fully define or implement processes for the use of Personal Identity Verification cards for logical access. This issue was identified in a previous audit, and the CSB plans to complete corrective actions to resolve the deficiency by March 31, 2020. *See Appendix A, FISMA Questions 24, 28 and 29.*
Respond	Incident Response	The CSB did not define incident response processes for the eradication of security incidents, as required by NIST, Special Publication 800-53, Revision 4, Security Control: Incident Response – 4. *See Appendix A, FISMA Question 55.*

Source: OIG analysis.

* Per 41 U.S.C. § 4713(k)(6), supply chain risk is defined as "the risk that any person may sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted on the covered articles."

Conclusion

The CSB would greatly improve and strengthen its cybersecurity program by fully defining the policies, procedures and strategies to manage supply chain risks and eradicate security incidents. Improvements in the CSB's supply chain management would allow the agency to guard against attacks on its network and keep critical resources available for end users. Likewise, improvements in the eradication of security incidents would greatly enhance the CSB's response capability and provide the agency with a consistent approach for eliminating root causes of security breaches once they are contained.

Recommendations

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

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

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.

CSB Response and OIG Assessment

The CSB agreed with our recommendations and provided acceptable planned corrective actions and milestone dates. The CSB stated it would update its Board Order 34, Information Technology Security Program, to document its risk management procedures by April 30, 2020. We consider this recommendation resolved with corrective action pending. The CSB stated it would update Appendix F of Board Order 34 to define and document its incident handling capabilities by January 31, 2020. The CSB provided documentation that it completed this corrective action. The CSB's complete response is in Appendix C.

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	5	Define and document risk management procedures for identifying, assessing and managing information technology supply chain risk.	R	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	4/30/20	
2	6	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.	C	Chairperson, U.S. Chemical Safety and Hazard Investigation Board	1/31/20	

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

OIG-Completed Department of Homeland Security CyberScope Template

Inspector General Section Report	2019 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 CM8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2019 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).

Defined (Level 2)

Comments: See remarks for question 13.2

2 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets 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 2019 CIO FISMA Metrics: 1.2 and 3.9.2; CSF: ID.AM-1).

Defined (Level 2)

Comments: See remarks for question 13.2

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: CA7, CM-8, and CM-10; NIST SP 800-137; NISTIR 8011; FEA Framework, v2; FY 2019 CIO FISMA Metrics: 3.10.1; CSF: ID.AM-2)?

Defined (Level 2)

Comments: See remarks for question 13.2

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 PM11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2019 CIO FISMA Metrics: 1.1; OMB M-19-03)?

Defined (Level 2)

Comments: See remarks for question 13.2

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)?

Ad Hoc (Level 1)

Comments: See remarks for question 13.2

Function 1: 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 (NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA9, SA-12, and PM-9; NIST SP 800-161; CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

Ad Hoc (Level 1)

Comments: See remarks for question 13.2

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 M19-03)?

Defined (Level 2)

Comments: See remarks for question 13.2

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)?

Defined (Level 2)

Comments: See remarks for question 13.2

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: See remarks for question 13.2

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: See remarks for question 13.2

Function 1: Identify - Risk Management

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: See remarks for question 13.2

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)?

Defined (Level 2)

Comments: See remarks for question 13.2

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

Defined (Level 2)

Comments: See remarks for question 13.2

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?

We limited our testing to determining 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 as Defined (Level 2). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

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: See remarks for question 22

Function 2A: Protect - Configuration Management

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: See remarks for question 22

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: See remarks for question 22

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 2019CIO FISMA Metrics: 1.1,2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7and PR.IP-1)?

Defined (Level 2)

Comments: See remarks for question 22

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, and SI-2; FY 2019CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1and DE.CM-8)?

Defined (Level 2)

Comments: See remarks for question 22

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 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20,Control 4.5; FY 2019CIO FISMA Metrics: 2.13; CSF: ID.RA-1; DHS Binding Operational Directive(BOD)15-01; DHS BOD 18-02)?

Defined (Level 2)

Comments: See remarks for question 22

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-08-05)?

Defined (Level 2)

Comments: See remarks for question 22

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 and CM-3; CSF: PR.IP-3).?

Defined (Level 2)

Comments: See remarks for question 22

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?

We limited our testing to determining 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 as Defined (Level 2). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

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: See remarks for question 32

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

Ad Hoc (Level 1)

Comments: See remarks for question 32

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: See remarks for question 32

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: See remarks for question 32

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: See remarks for question 32

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)?

Ad Hoc (Level 1)

Comments: See remarks for question 32

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)?

Ad Hoc (Level 1)

Comments: See remarks for question 32

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: See remarks for question 32

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: See remarks for question 32

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?

We limited our testing to determining 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 as Defined (Level 2). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

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: See remarks in question 38

Function 2C: Protect - Data Protection and Privacy

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: See remarks in question 38

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: See remarks in question 38

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: See remarks in question 38

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)

Defined (Level 2)

Comments: See remarks in question 38

Function 2C: Protect - Data Protection and Privacy

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?

We limited our testing to determining 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 as Defined (Level 2). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

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: See remarks in question 45.2

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: See remarks in question 45.2

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: See remarks in question 45.2

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).

Defined (Level 2)

Comments: See remarks in question 45.2

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: See remarks in question 45.2

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)?

Defined (Level 2)

Comments: See remarks in question 45.2

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

Defined (Level 2)

Comments: See remarks in question 45.2

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?

We limited our testing to determining 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 as Defined (Level 2). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

Calculated Maturity Level - Defined (Level 2)

Function 3: Detect - ISCM

Function 3: Detect - 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: See remarks in question 51.2

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: See remarks in question 51.2

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: See remarks in question 51.2

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: See remarks in question 51.2

50 How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?

Defined (Level 2)

Comments: See remarks in question 51.2

51.1 Please provide the assessed maturity level for the agency's Detect Function.

Defined (Level 2)

Comments: See remarks in question 51.2

Function 3: Detect - ISCM

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?

We limited our testing to determining 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 as Defined (Level 2). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

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: See remarks in question 59.2

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: See remarks in question 59.2

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: See remarks in question 59.2

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)

Ad Hoc (Level 1)

Comments: See remarks in question 59.2

Function 4: Respond - Incident Response

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: See remarks in question 59.2

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: See remarks in question 59.2

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: See remarks in question 59.2

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

Defined (Level 2)

Comments: See remarks in question 59.2

Function 4: Respond - Incident Response

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?

We limited our testing to determining 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 as Defined (Level 2). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

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)?

Defined (Level 2)

Comments: See remarks in question 67.2

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: See remarks in question 67.2

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: See remarks in question 67.2

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: See remarks in question 67.2

Function 5: Recover - Contingency Planning

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)?

Defined (Level 2)

Comments: See remarks in question 67.2

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: See remarks in question 67.2

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: See remarks in question 67.2

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

Defined (Level 2)

Comments: See remarks in question 67.2

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?

We limited our testing to determining 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 as Defined (Level 2). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

Calculated Maturity Level - Defined (Level 2)

Function 0: Overall

Function 0: Overall

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

Effective

Comments:

CSB has demonstrated it has defined policies, procedures and strategies for all five of the information security function areas. The Office of the Inspector General assessed the five Cybersecurity Framework function areas and concluded that CSB has achieved an overall maturity Level 2, Defined, which denotes that the agency has formalized documented policies, procedures and strategies, in adherence to the FY 2019 Inspector General Federal Information Security Modernization Act reporting metrics. While CSB has policies, procedures and strategies for these function areas and domains, improvements are still needed in the following areas: Risk Management - CSB neither identified nor defined its risk management procedures for identifying, assessing or managing supply chain risk. Incident Response - CSB did not define incident handling processes specific to eradication in its incident response procedures. Identity and Access Management - CSB has not completed its corrective actions to implement processes for the use of Personal Identity Verification cards for the logical access of privileged and non-privileged users.

Function 0: Overall

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

CSB has demonstrated it has defined policies, procedures and strategies for all five of the information security function areas. The Office of the Inspector General assessed the five Cybersecurity Framework function areas and concluded that CSB has achieved an overall maturity Level 2, Defined, which denotes that the agency has formalized documented policies, procedures and strategies, in adherence to the FY 2019 Inspector General Federal Information Security Modernization Act reporting metrics.

While CSB has policies, procedures and strategies for these function areas and domains, improvements are still needed in the following areas:

Risk Management - CSB neither identified nor defined its risk management procedures for identifying, assessing or managing supply chain risk.
Incident Response - CSB did not define incident handling processes specific to eradication in its incident response procedures.
Identity and Access Management - CSB has not completed its corrective actions to implement processes for the use of Personal Identity Verification cards for the logical access of privileged and non-privileged users.

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	2
Defined	10
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	0
Defined	8
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	3
Defined	6
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	0
Defined	5
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	0
Defined	6
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	5
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)Not Effective	

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	1
Defined	6
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	0
Defined	7
Consistently Implemented	0
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)	See remarks for question 13.2
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Defined (Level 2)	Defined (Level 2)	See remarks in question 45.2
Function 3: Detect - ISCM	Defined (Level 2)	Defined (Level 2)	See remarks in question 51.2
Function 4: Respond - Incident Response	Defined (Level 2)	Defined (Level 2)	See remarks in question 59.2
Function 5: Recover - Contingency Planning	Defined (Level 2)	Defined (Level 2)	See remarks in question 67.2
Overall	Not Effective	Effective	CSB has demonstrated it has defined policies, procedures and strategies for all five of the information security function areas. The Office of the Inspector General assessed the five Cybersecurity Framework function areas and concluded that CSB has achieved an overall maturity Level 2, Defined, which denotes that the agency has formalized documented policies, procedures and strategies, in adherence to the FY 2019 Inspector General Federal Information Security Modernization Act reporting metrics. While CSB has policies, procedures and strategies for these function areas and domains, improvements are still needed in the following areas: Risk Management - CSB neither identified nor defined its risk management procedures for identifying, assessing or managing supply chain risk. Incident Response - CSB did not define incident handling processes specific to eradication in its incident response procedures. Identity and Access Management - CSB has not completed its corrective actions to implement processes for the use of Personal Identity Verification cards for the logical access of privileged and non-privileged users.

Appendix B

Status of CSB Corrective Actions for FY 2018 FISMA Audit Recommendations

The below table details the OIG's analysis of the corrective actions that the CSB has implemented for the recommendations issued in OIG Report No. 19-P-0147, *CSB Still Needs to Improve Its "Incident Response" and "Identity and Access Management" Information Security Functions*, dated May 9, 2019.

Recommendation		Corrective action	OIG analysis of corrective action status
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.	The CSB has identified the necessary software and settings in its Active Directory and Group Policy configuration and will work towards enabling Personal Identity Verification login for those employees with domain administrative responsibilities. The CSB provided evidence that settings for domain administrators were updated on October 24, 2019, to require multifactor authentication, with full implementation for all users to be completed by March 31, 2020.	**Open.** Corrective actions in process. **Planned Completion Date: 3/31/20**
2	Document policies and procedures for data exfiltration and enhanced network defenses, as required by National Institute of Standards and Technology Special Publication 800-53 (specifically, the "System and Information Integrity" control).	The CSB thoroughly documented its system integrity controls, specifically according to NIST Special Publication 800-53, SI-1 (System and Information Integrity Policy and Procedures) and SI-4 (Information System Monitoring, specifically SI-4(4) and SI-4(8)), in the Information System Security Plan.	**Completed on 5/30/19**
3	Define and document incident handling policies and procedures that address containment, eradication and recovery, as required by National Institute of Standards and Technology Special Publication 800-53 (specifically, the "Incident Response" control).	The CSB reviewed and revised the Information System Contingency Plan of the General Support System—which addresses data security, integrity, backup, recovery and reconstitution—and the Incident Response policy in Appendix F of Board Order 34, Information Technology Security Program.	**Completed on 5/17/19**

Recommendation		Corrective action	OIG analysis of corrective action status
4	Document and formalize within the CSB policies and procedures the agency's rationale for not having an automated system for the detection of potential incidents.	The CSB is a micro-agency with a limited number of systems. System logging can generate alerts from firewalls, antimalware and antispam software, and server event log (see Recommendation 5 for more detail), but the agency does not maintain a centralized system for detecting incidents across all systems. The CSB documented more thoroughly in the Information System Security Plan where and how these logging capabilities, alerts and records are generated and kept.	**Completed on 5/30/19**
5	Document established procedures to generate alerts based on log data analysis and to record pertinent data for suspicious activity.	The CSB's systems record events and activity through various system logging capabilities—antispam logging, malware defense logs, Windows event logs, Cisco ASA firewall logs, application event logs and so on. Some of those generate alerts based on unusual activity. The CSB documented more thoroughly in the Information System Security Plan where and how these logging capabilities, alerts and records are generated and kept.	**Completed on 5/30/19**

Source: OIG analysis.

Appendix C

CSB Response to Draft Report

U.S. Chemical Safety and Hazard Investigation Board

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

Honorable Kristen M. Kulinowski
Interim Executive Authority

Honorable Manny Ehrlich, Jr.
Board Member

Honorable Rick Engler
Board Member

November 20, 2019

Mr. Rudy M. Brevard
Director, Information Resources Management Directorate
Office of Inspector General
Office of Audit and Evaluation
U.S. Environmental Protection Agency
Washington, DC 20460

Dear Mr. Brevard:

Thank you for the opportunity to review the FY2019 Federal Information Security Modernization Act (FISMA) draft report entitled "CSB Needs to Improve Its "Risk Management," "Identity and Access Management," and "Incident Response" Information Security Functions (Project # OA&E-FYI 9-0213.

The Chemical Safety Board (CSB) acknowledges the two recommendations identified in the FISMA report and offer the following comments and observations with respect to the recommendations identified:

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

The CSB concurs with this finding. The CSB will more thoroughly document its risk management procedures as regards supply chain risk, in a new section of Board Order 34, Information Technology Security Program.

Expected Completion Date: April 30, 2020

Recommendation #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 concurs with this finding. The CSB will more thoroughly document its incident handling procedures, specifically in the area of eradication and verification, in Appendix F of Board Order 34, Information Technology Security Program.

Expected Completion Date: January 31, 2020

Thank you again for the opportunity to provide our comments to this report. If you have any questions regarding our responses, please contact our OIG Liaison, Ms. Anna Brown, at (202) 261-7639.

Sincerely,

Dr. Kristen M. Kulinowski
Interim Executive Authority

Appendix D

Distribution

Chairperson and Member, 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