U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

U.S. Chemical Safety Board

Improvements Needed in CSB's Identity and Access Management and Incident Response Security Functions

Report No. 18-P-0030 October 30, 2017

Report Contributors:

Rudolph M. Brevard
Iantha Maness
Christina Nelson
Jeremy Sigel
Sabrena Stewart

Abbreviations

CSB	U.S. Chemical Safety and Hazard Investigation Board
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG	Inspector General
OIG	Office of Inspector General
U.S.C.	United States Code

Cover image: Personal Identity Verification Authentication. (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, DC 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, DC 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

18-P-0030
October 30, 2017

At a Glance

Why We Did This Review

We performed this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) security practices related to performance measures outlined in the fiscal year 2017 Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA). The reporting metrics outline five maturity levels for IGs to rate their agency's information security programs:

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

We reported our audit results using the CyberScope system developed by the U.S. Department of Homeland Security, which calculates the effectiveness of the agency's information security program.

This report addresses the following CSB goal:

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

Send all inquiries to our public affairs office at (202) 566-2391 or visit www.epa.gov/oig.

Listing of OIG reports.

Improvements Needed in CSB's Identity and Access Management and Incident Response Security Functions

What We Found

Weaknesses in the Identity and Access Management and Incident Response metric domains leave the CSB vulnerable to attacks occurring and not being detected in a timely manner.

We rated CSB's information security program at Level 2 (Defined) for all five Cybersecurity Framework Security Function areas and corresponding metric domains assessed as specified by the fiscal year 2017 IG FISMA Reporting Metrics:

1. Identify – Risk Management.
2. Protect – Configuration Management, Identity and Access Management, and Security Training.
3. Detect – Information Security Continuous Monitoring.
4. Respond – Incident Response.
5. Recover – Contingency Planning.

We tested whether the CSB developed policies, procedures and strategies for each area within the reporting metric. If the CSB developed policies, procedures and strategies consistent with the reporting metric question, we rated the agency at Level 2 (Defined).

We also conducted additional testing of CSB's patch management processes under the Configuration Management domain to determine whether the agency implemented the noted policies, procedures and strategies. We concluded that CSB's patch management processes graduated to a Level 5 (Optimized) maturity level rating.

While CSB has policies, procedures and strategies for many of the Cybersecurity Framework Security Function areas and corresponding metric domains, CSB lacks guidance and needs improvement in the following areas:

- **Identity and Access Management** – CSB does not include fully defined processes for Personal Identity Verification card technology for physical and logical access.

- **Incident Response** – CSB does not include fully defined incident response processes or technologies to respond to cybersecurity events.

Appendix A contains the results for the fiscal year 2017 IG FISMA Reporting Metrics. We worked closely with CSB throughout the audit to keep them apprised of our findings. We met with CSB on September 14, 2017, to brief them on our final results, and CSB agreed with our conclusions.

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

THE INSPECTOR GENERAL

October 30, 2017

The Honorable Vanessa Allen Sutherland
Chairperson and Member
U.S. Chemical Safety and Hazard Investigation Board
1750 Pennsylvania Avenue NW, Suite 910
Washington, D.C. 20006

Dear Ms. Sutherland:

This is our report on the audit of the U.S. Chemical Safety and Hazard Investigation Board's implementation of the information security policies and practices outlined by the 2017 Inspector General Reporting Metrics under the Federal Information Security Modernization Act of 2014. This report contains findings that describe the issues the Office of Inspector General has identified.

You are not required to provide a written response to this final report. In accordance with Office of Management and Budget reporting instructions for the Federal Information Security Modernization Act, we are forwarding this report to the Director of the Office of Management and Budget.

We will post this report to our website at www.epa.gov/oig.

Sincerely,

Arthur A. Elkins Jr.

Table of Contents

Appendices

Purpose

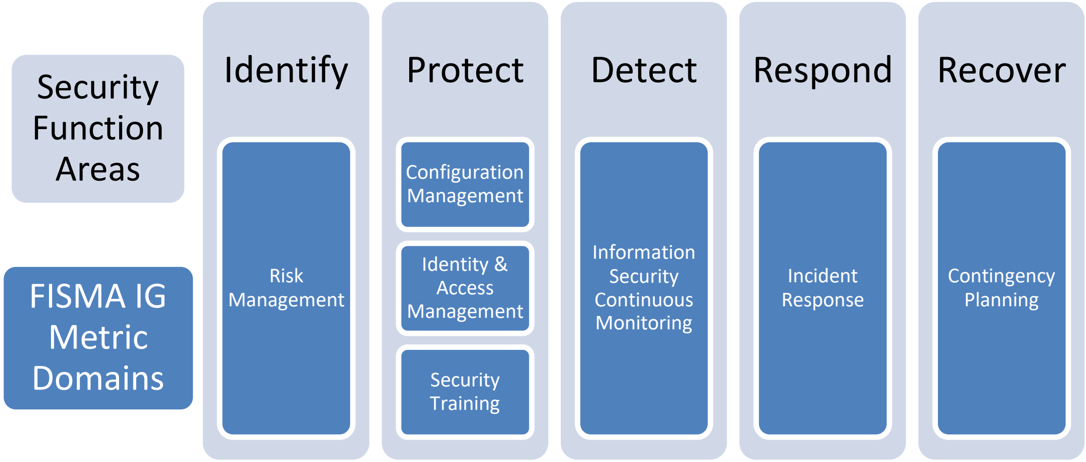
The Office of Inspector General (OIG) performed this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) security practices related to performance measures, as outlined in the fiscal year (FY) 2017 Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA).

Background

Under FISMA (44 U.S.C. § 3544(a)(1)(A)), 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.

The FY 2017 IG FISMA Reporting Metrics identified domains within the five security functions in the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, as shown in Figure 1.

Figure 1: Cybersecurity framework security function areas and corresponding IG FISMA Reporting Metric domains



Source: OIG graphic.

The effectiveness of the information security program is based on a maturity model spectrum in which the lower maturity level must be met before the next maturity level can be evaluated. This ensures that the agencies have developed policies and procedures, while advanced levels describe the extent to which the agencies have institutionalized those policies and procedures.

There are five maturity model levels, as follows:

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

This year's FISMA metrics represent a significant departure from prior year's reporting metrics. This year, the Office of Management and Budget introduced a new maturity model rating system for three of the five function areas (Identify, Protect and Recover). The Office of Management and Budget also reorganized the model to make them more intuitive. Because of these changes, this year's results cannot be compared to prior ratings of the security function areas.

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 up to the event and identify the cause or causes so that similar events might be prevented. CSB is headquartered in Washington, D.C., and its Western Regional Office is in Denver, Colorado. The CSB's staff includes investigators, engineers, safety experts, attorneys and administrators.

CSB investigated a 2017 explosion in a gasoline processing unit. (CSB photo)

Responsible Offices

The CSB's Board Chairperson is responsible for agency administration. The CSB's Office of Administration is responsible for the information technology security program. The Chief Information Officer is responsible for making risk management decisions regarding deficiencies; their potential impact on controls; and the confidentiality, integrity and availability of systems. The Chief Information Officer is also responsible for reporting to the agency head on progress of remedial actions on the agency information security program.

Scope and Methodology

We conducted this audit from May to October 2017 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 the Ad Hoc Maturity Level (Level 1) for each question in the FY 2017 IG FISMA Reporting Metrics. Descriptions of the maturity levels are in Table 1.

Table 1: Maturity level descriptions

Maturity level	Maturity level description
Level 1: Ad Hoc	Policies, procedures and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures and strategy 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 2017 IG FISMA Reporting Metrics.

We tested 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).

Additional testing was conducted on the patch management process under Question #19 of the Configuration Management metric domain to determine whether the agency implemented the noted patch management policies, procedures and strategies to achieve a maturity level higher than Level 2 (Defined).

We collected management's feedback on the analysis through weekly emails. We worked closely with CSB and briefed them on the audit results for each function area of the FISMA metrics.

Prior Audit

During our testing of CSB's FY 2017 FISMA compliance, we followed up on weaknesses identified in the FY 2016 FISMA Report No. 17-P-0045, *CSB Has Effective "Identify" and" Recover" Information Security Functions, but Attention Is Needed in Other Information Security Function Areas*, dated November 14, 2016. We reported that CSB needed improvements in the Identity and Access

Management, Security Training, and Incident Response security function areas and corresponding metrics. While improvements were made in the Security Training program to provide relevant personnel with social engineering and phishing exercises and track training requirements, weaknesses in the Identity and Access Management and Incident Response function areas remained.

Results of Review

The CSB's information security program is assessed overall at the Level 2 – Defined maturity level, as specified in the FY 2017 IG FISMA reporting. We also conducted additional testing of CSB's patch management process under the Configuration Management domain to determine whether the agency implemented the noted patch management policies, procedures and strategies to achieve a higher maturity level. We determined that CSB's patch management program was operating at the Level 5 – Optimized maturity level.

Table 2: Maturity level of CSB's information security function areas

Function area	Function domains	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	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: FY17 IG FISMA Reporting Metrics.

Several areas within the CSB's information security program were identified as receiving a Level 1 (Ad Hoc) response, which affected the agency's rating and ability to achieve Level 4 of the maturity model. Based on our analysis, improvements are needed in the following security function areas and corresponding metric domains:

- **"Protect" Function Area:**
  - **Identity and Access Management:** CSB does not include fully defined processes for the use of Personal Identity Verification cards for physical and logical access.

- **"Respond" Function Area:**
  - **Incident Response:** CSB does not include fully defined incident response processes or technologies to respond to cybersecurity events.

Appendix A provides the responses for each FISMA metric section.

Appendix A

Department of Homeland Security CyberScope Template

Inspector General

Section Report

2017

Annual FISMA Report

Chemical Safety Board

Function 1: Identify - Risk Management

1 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: CA-3 and PM-5; OMB M-04-25; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4)?

Defined (Level 2)

Comments: See remarks in 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: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2)?

Defined (Level 2)

Comments: See remarks in 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: CA-7, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?

Defined (Level 2)

Comments: See remarks in 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 (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; and FIPS 199)?

Defined (Level 2)

Comments: See remarks in question 13.2

Function 1: Identify - Risk Management

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that include 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 800-39; NIST 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; CFO Council ERM Playbook)?

Defined (Level 2)

Comments: See remarks in question 13.2

6 Has the organization defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture to provide a disciplined and structured methodology for managing risk (NIST 800-39; FEA; NIST 800-53: PL-8, SA-3, and SA-8)?

Defined (Level 2)

Comments: See remarks in question 13.2

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST 800-39: Section 2.3.1 and 2.3.2; NIST 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2, OMB A-123, CFO Council ERM Playbook)?

Defined (Level 2)

Comments: See remarks in 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: CA-5; OMB M-04-25)?

Defined (Level 2)

Comments: See remarks in question 13.2

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) selecting and implementing security controls to mitigate system-level risks (NIST 800--37; NIST 800-39; NIST 800--53: PL-2, RA-1; NIST 800-30; CSF:ID.RA-1 – 6)?

Defined (Level 2)

Comments: See remarks in 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)?

Defined (Level 2)

Comments: See remarks in question 13.2

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 (FAR Case 2007--004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, 52.239-1; President's Management Council; NIST 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2017 CIO FISMA Metrics: 1.7, 1.8)?

Defined (Level 2)

Comments: See remarks in 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 in question 13.2

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: See remarks in 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 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). 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.

Comments: We limited our testing 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). 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: CM-1; SP 800-128: Section 2.4)?

Defined (Level 2)

Comments: See remarks in 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 location within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contracted systems (NIST 800--128: Section 2.3.2; NIST 800--53: CM-9)?

Defined (Level 2)

Comments: See remarks in 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: CM-1; NIST 800-128: 2.2.1)

Defined (Level 2)

Comments: See remarks in 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: CM-2, CM-8; FY 2017 CIO FISMA Metrics: 1.4, 1.5, and 2.1; CSF: ID.DE.CM-7)?

Defined (Level 2)

Comments: See remarks in question 22

18 To what extent does the organization utilize configuration settings/common secure configurations for its information systems (NIST SP 800-53: CM-6, CM-7, and SI-2; FY 2017 CIO FISMA Metrics: 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Defined (Level 2)

Comments: See remarks in question 22

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53: CM-3, SI-2; NIST 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20 Control 4.5; and DHS Binding Operational Directive 15-01)?

Optimized (Level 5)

Comments: See remarks in question 22

Function 2A: Protect - Configuration Management

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (FY 2017 CIO Metrics: 2.26, 2.27, 2.29; OMB M-08-05)?

Defined (Level 2)

Comments:

See remarks in question 22

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 800-53: CM--2, CM-3)?

Defined (Level 2)

Comments:

See remarks in 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 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). Additional testing was conducted for the Patch Management process under Question #19 to determine whether the agency implemented the noted patch management policies, procedures and strategies to achieve a higher maturity level. This process was found to be effective as implemented and rated at Level 5 - Optimized.

Comments:

We limited our testing 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). Additional testing was conducted for the Patch Management process under Question #19 to determine whether the agency implemented the noted patch management policies, procedures and strategies to achieve a higher maturity level. This process was found to be effective as implemented and rated at Level 5 - Optimized.

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 800-53: AC-1, IA-1, PS-1; and the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Defined (Level 2)

Comments: See remarks in 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 in question 32

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 27 through 31) (NIST 800-53: AC-1 and IA--1; Cybersecurity Strategy and Implementation Plan (CSIP); and SANS/CIS Top 20: 14.1)?

Defined (Level 2)

Comments: See remarks in 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: PS-2, PS- 3; and National Insider Threat Policy)?

Defined (Level 2)

Comments: See remarks in 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: AC-8, PL-4, and PS-6)?

Defined (Level 2)

Comments: See remarks in question 32

Function 2B: Protect - Identity and Access Management

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: AC-8, PL-4, and PS-6)?

Defined (Level 2)

Comments: See remarks in question 32

28 To what extent has the organization implemented strong authentication mechanisms (PIV or 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: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

Ad Hoc (Level 1)

Comments: See remarks in question 32

29 To what extent has the organization implemented strong authentication mechanisms (PIV or 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: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

Ad Hoc (Level 1)

Comments: See remarks in question 32

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 2017 CIO FISMA metrics: Section 2; NIST SP 800-53: AC-1, AC-2 (2), AC-17; CSIP)?

Defined (Level 2)

Comments: See remarks in question 32

Function 2B: Protect - Identity and Access Management

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: AC--17, SI-4; and FY 2017 CIO FISMA Metrics: Section 2)?

Defined (Level 2)

Comments:

See remarks in 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 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). 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.

Comments:

We limited our testing 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). 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 - Security Training

Function 2C: Protect - Security Training

33 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 800-53: AT-1; and NIST SP 800-50)?

Defined (Level 2)

Comments:

See remarks in question 39.2

34 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 800-53: AT-2 and AT-3; NIST 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181 (Draft); and CIS/SANS Top 20: 17.1)?

Defined (Level 2)

Comments:

See remarks in question 39.2

35 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 800--53: AT-1; NIST 800-50: Section 3))

Defined (Level 2)

Comments:

See remarks in question 39.2

36 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 questions 37 and 38 below) (NIST 800-53: AT-1 through AT-4; and NIST 800-50)

Defined (Level 2)

Comments:

See remarks in question 39.2

Function 2C: Protect - Security Training

37 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 800-53: AT-2; FY 17 CIO FISMA Metrics: 2.23; NIST 800-50: 6.2; SANS Top 20: 17.4)

Defined (Level 2)

Comments: See remarks in question 39.2

38 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 800-53: AT-3 and AT-4; FY 17 CIO FISMA Metrics: 2.23)?

Defined (Level 2)

Comments: See remarks in question 39.2

39.1 Please provide the assessed maturity level for the agency's Protect - Configuration Management/Identity and Access Management/Security Training (Functions 2A - 2C).

Defined (Level 2)

Comments: See remarks in Question 39.2

Function 2C: Protect - Security Training

39.2 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 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). 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.

Comments:

We limited our testing 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). 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

40 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 organization-wide approach to ISCM (NIST SP 800-137: Sections 3.1 and 3.6)?

Defined (Level 2)

Comments:

See remarks in question 45.2

41 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; collecting 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: CA-7). (Note: The overall maturity level should take into consideration the maturity of question 43)

Defined (Level 2)

Comments:

See remarks in question 45.2

Function 3: Detect - ISCM

42 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: CA-1; NIST SP 800-137; and FY 2017 CIO FISMA Metrics)?

Defined (Level 2)

Comments: See remarks in question 45.2

43 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: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?

Defined (Level 2)

Comments: See remarks in question 45.2

44 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 45.2

45.1 Please provide the assessed maturity level for the agency's Detect - ISCM 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 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 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). 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.

Comments: We limited our testing 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). 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

46 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: IR-1; NIST 800-61 Rev. 2; FY 2017 CIO FISMA Metrics: 4.1, 4.3, and 4.6)? (Note: The overall maturity level should take into consideration the maturity of questions 48 - -52)

Ad Hoc (Level 1)

Comments: See remarks in question 53.2

47 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; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-16-03; OMB M-16-04; FY 2017 CIO FISMA Metrics: 1.6 and 4.5; and US-CERT Federal Incident Notification Guidelines)?

Defined (Level 2)

Comments: See remarks in question 53.2

48 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; US- CERT Incident Response Guidelines)?

Defined (Level 2)

Comments: See remarks in question 53.2

49 How mature are the organization's processes for incident handling (NIST 800-53: IR-4)?

Ad Hoc (Level 1)

Comments: See remarks in question 53.2

50 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-16-03; NIST 800-53: IR-6; US-CERT Incident Notification Guidelines)?

Defined (Level 2)

Comments: See remarks in question 53.2

Function 4: Respond - Incident Response

51 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 and enter into contracts, as appropriate, for incident response support (FY 2017 CIO FISMA Metrics: 4.4; NIST SP 800-86)?

Defined (Level 2)

Comments: See remarks in question 53.2

52 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)

Ad Hoc (Level 1)

Comments: See remarks in question 53.2

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

Defined (Level 2)

Comments: See remarks in Question 53.2

Function 4: Respond - Incident Response

53.2 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 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). 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.

Comments:

We limited our testing 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). 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

54 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 800-53: CP-1 and CP-2; NIST 800-34; NIST 800-84; FCD-1: Annex B)?

Defined (Level 2)

Comments:

See remarks in question 61.2

55 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 56-60) (NIST SP 800-34; NIST SP 800--161).

Defined (Level 2)

Comments:

See remarks in question 61.2

Function 5: Recover - Contingency Planning

56 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST 800-53: CP-2; NIST 800--34, Rev. 1, 3.2, FIPS 199, FCD--1, OMB M-17-09)?

Defined (Level 2)

Comments: See remarks in question 61.2

57 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST 800-53: CP-2; NIST 800-34)?

Defined (Level 2)

Comments: See remarks in question 61.2

58 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST 800-34; NIST 800-53: CP-3, CP-4)?

Defined (Level 2)

Comments: See remarks in question 61.2

59 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST 800--53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD1; NIST CSF: PR.IP- 4; and NARA guidance on information systems security records)?

Defined (Level 2)

Comments: See remarks in question 61.2

60 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 800-53: CP-2, IR-4)?

Defined (Level 2)

Comments: See remarks in question 61.2

Function 5: Recover - Contingency Planning

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

Defined (Level 2)

Comments: See remarks in question 61.2

61.2 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 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). 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.

Comments: We limited our testing 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). 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)

Comments: CSB has demonstrated they have defined policy, procedures, and strategies for all five of the five information security function areas. The Office of the Inspector General (OIG) assessed the five Cybersecurity Framework function areas in adherence to the FY 2017 Inspector General (IG) Federal Information Security Modernization Act (FISMA) reporting metrics. If the policies, procedures, and strategies were formalized and documented the agency was rated at Level 2 (Defined). If not, we rated the agency at Level 1 (Ad Hoc). Additional testing was conducted for the Patch Management process under Question #19 to determine whether the agency implemented the noted patch management policies, procedures, and strategies to achieve a higher maturity level. This process was found to be effective as implemented and rated at Level 5 - Optimized. Several areas within the CSB's information security program were identified at Level 1 – Ad Hoc. Based on our analysis improvements are needed in the following areas: • Identity and Access Management: CSB has not fully implemented the use of Personal Identity Verification cards for physical and logical access. • Incident Response: CSB has not identified nor fully defined its incident response processes or technologies to respond to cybersecurity events.

Function 0: Overall

Function 0: Overall

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

Effective

Comments: CSB has demonstrated they have defined policy, procedures and strategies for all five of the five information security function areas. The Office of the Inspector General (OIG) assessed the five Cybersecurity Framework function areas in adherence to the FY 2017 Inspector General (IG) Federal Information Security Modernization Act (FISMA) reporting metrics. If the policies, procedures and strategies were formalized and documented the agency was rated at Level 2 (Defined). Additional testing was conducted for the Patch Management process under Question #19 to determine whether the agency implemented the noted patch management policies, procedures and strategies to achieve a higher maturity level. This process was found to be effective as implemented and rated at Level 5 - Optimized. Several areas within the CSB's information security program were identified at Level 1 – Ad Hoc. Based on our analysis, improvements are needed in the following areas: • Identity and Access Management: CSB has not fully implemented the use of Personal Identity Verification cards for physical and logical access. • Incident Response: CSB has not identified nor fully defined its incident response processes or technologies to respond to cybersecurity events.

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.

CSB has demonstrated they have defined policy, procedures and strategies for all five of the five information security function areas. The Office of the Inspector General (OIG) assessed the five Cybersecurity Framework function areas in adherence to the FY 2017 Inspector General (IG) Federal Information Security Modernization Act (FISMA) reporting metrics. If the policies, procedures and strategies were formalized and documented the agency was rated at Level 2 (Defined). If not, we rated the agency at Level 1 (Ad Hoc). Additional testing was conducted for the Patch Management process under Question #19 to determine whether the agency implemented the noted patch management policies, procedures and strategies to achieve a higher maturity level. This process was found to be effective as implemented and rated at Level 5 - Optimized. Several areas within the CSB's information security program were identified at Level 1 – Ad Hoc. Based on our analysis, improvements are needed in the following areas:

- **Identity and Access Management: CSB does not include fully defined processes for Personal Identity Verification card technology for physical and logical access.**

- **Incident Response: CSB has not identified nor fully defined its incident response processes or technologies to respond to cybersecurity events.**

Function 0: Overall

Comments:

CSB has demonstrated they have defined policy, procedures and strategies for all five of the five information security function areas. The Office of the Inspector General (OIG) assessed the five Cybersecurity Framework function areas in adherence to the FY 2017 Inspector General (IG) Federal Information Security Modernization Act (FISMA) reporting metrics. If the policies, procedures and strategies were formalized and documented the agency was rated at Level 2 (Defined). If not, we rated the agency at Level 1 (Ad Hoc). Additional testing was conducted for the Patch Management process under Question #19 to determine whether the agency implemented the noted patch management policies, procedures and strategies to achieve a higher maturity level. This process was found to be effective as implemented and rated at Level 5 - Optimized. Several areas within the CSB’s information security program were identified at Level 1 – Ad Hoc. Based on our analysis, improvements are needed in the following areas:

- Identity and Access Management:CSB does not include fully defined processes for Personal Identity Verification cards for physical and logical access
- Incident Response: CSB has not identified nor fully defined its incident response processes or technologies to respond to cybersecurity events

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	12
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0
Defined	7
Consistently Implemented	0
Managed and Measurable	0
Optimized	1
Function Rating: Defined (Level 2)	0

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)	0

Function 2C: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	6
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

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)	0

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	3
Defined	4
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

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)	0

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 in Question 13.2
Function 2: Protect - Configuration Management / Identity Management / Security Training	Defined (Level 2)	Defined (Level 2)	See remarks in Question 39.2
Function 3: Detect - ISCM	Defined (Level 2)	Defined (Level 2)	See remarks in Question 45.2
Function 4: Respond - Incident Response	Defined (Level 2)	Defined (Level 2)	See remarks in Question 53.2
Function 5: Recover - Contingency Planning	Defined (Level 2)	Defined (Level 2)	See remarks in question 61.2

Overall	Not Effective	Effective	CSB has demonstrated they have defined policy, procedures, and strategies for all five of the five information security function areas. The Office of the Inspector General (OIG) assessed the five Cybersecurity Framework function areas in adherence to the FY 2017 Inspector General (IG) Federal Information Security Modernization Act (FISMA) reporting metrics. If the policies, procedures, and strategies were formalized and documented the agency was rated at Level 2 (Defined). If not, we rated the agency at Level 1 (Ad Hoc). Additional testing was conducted for the Patch Management process under Question #19 to determine whether the agency implemented the noted patch management policies, procedures, and strategies to achieve a higher maturity level. This process was found to be effective as implemented and rated at Level 5 - Optimized. Several areas within the CSB's information security program were identified at Level 1 – Ad Hoc. Based on our analysis improvements are needed in the following areas: • Identity and Access Management: CSB has not fully implemented the use of Personal Identity Verification cards for physical and logical access. • Incident Response: CSB has not identified nor fully defined its incident response processes or technologies to respond to cybersecurity events.

Appendix B

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