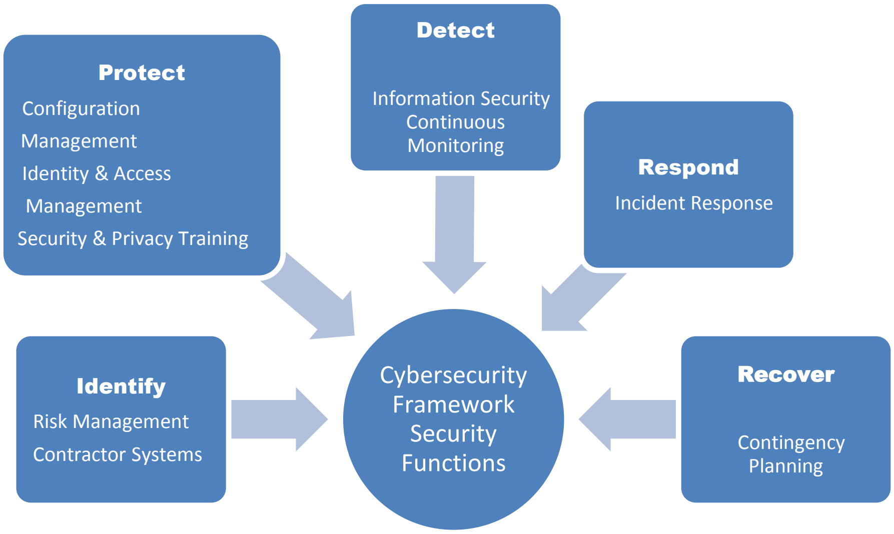
U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

U.S. Chemical Safety Board

CSB Has Effective “Identify” and “Recover” Information Security Functions, but Attention Is Needed in Other Information Security Function Areas

Report No. 17-P-0045 **November 14, 2016**



Protect
Configuration Management
Identity & Access Management
Security & Privacy Training

Detect
Information Security Continuous Monitoring

Respond
Incident Response

Identify
Risk Management
Contractor Systems

Cybersecurity Framework Security Functions

Recover
Contingency Planning

Report Contributors:

Rudolph M. Brevard
Charles M. Dade
Nancy Dao
Nii-Lantei Lamptey
Iantha Maness

Abbreviations

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

Cover photo: Cybersecurity Framework Security Functions and FY 2016 Inspector General FISMA reporting metrics. (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

17-P-0045
November 14, 2016

At a Glance

Why We Did This Review

The Office of Inspector General (OIG) performed this audit to document and selectively test the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) security practices related to performance measures, as outlined in the fiscal year 2016 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) reporting metrics, and to follow up on the status of prior-year audit recommendations.

FISMA requires the OIG to annually evaluate its respective agency's information security program designed to protect the operations and assets of the agency.

We reported our audit results using the CyberScope system developed by the Department of Homeland Security. CyberScope calculates the effectiveness of an agency's information security program based on the responses to the FISMA reporting metrics.

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.

CSB Has Effective "Identify" and "Recover" Information Security Functions, but Attention Is Needed in Other Information Security Function Areas

What We Found

Two of the five information security function areas at CSB are considered effective. We assessed the following five Cybersecurity Framework Security Function areas and the corresponding metric domains as specified by the fiscal year 2016 Inspector General FISMA reporting metrics:

More work is needed by CSB to achieve an overall managed and measurable information security program that can effectively manage cybersecurity risks.

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

We evaluated each security function area using the maturity model. The maturity model is a tool to summarize the status of an agency's information security program and to outline what still needs to be done to improve the program. The maturity model assesses each function area as: Level 1 - Ad-hoc, Level 2 - Defined, Level 3 - Consistently Implemented, Level 4 - Managed and Measurable, or Level 5 - Optimized.

The maturity model defines the requirements to meet a particular maturity level, and CSB must meet all the requirements of that level before it can progress to the next higher level within the maturity model. The CSB would need to achieve Level 4 (Managed and Measurable) for a function area to be considered effective. The table below summarizes each function area the CSB achieved.

CSB's information security function area maturity

Security function areas	Maturity level rating
Identify and Recover	Level 5
Protect and Detect	Level 3
Respond	Level 2

Source: OIG testing results.

Additionally, CSB completed the 10 open recommendations from prior reports.

Appendix A contains the results for the fiscal year 2016 Inspector General FISMA reporting metrics. We met with CSB and updated our results based on additional information provided. CSB agreed with our results.

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

THE INSPECTOR GENERAL

November 14, 2016

The Honorable Vanessa Allen Sutherland
Chairperson and Board 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 2016 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

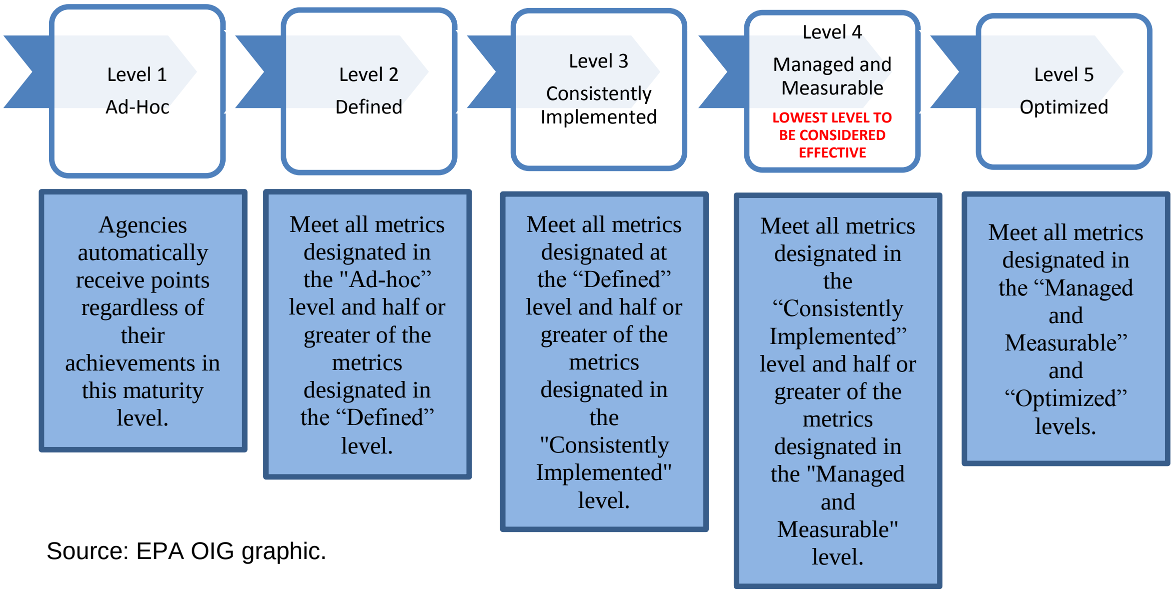
The Office of Inspector General (OIG) performed this audit to document and selectively test the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) security practices related to performance measures, as outlined in the fiscal year (FY) 2016 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) reporting metrics, and to follow up on the status of prior-year audit recommendations.

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.

Per FY 2016 Inspector General FISMA reporting metrics, there are five levels of maturity (see Figure 1 below) for each Cybersecurity Framework Function.

Figure 1: Progression of maturity levels



Level 1 Ad-Hoc

Agencies automatically receive points regardless of their achievements in this maturity level.

Level 2 Defined

Meet all metrics designated in the "Ad-hoc" level and half or greater of the metrics designated in the "Defined" level.

Level 3 Consistently Implemented

Meet all metrics designated at the "Defined" level and half or greater of the metrics designated in the "Consistently Implemented" level.

Level 4 Managed and Measurable

LOWEST LEVEL TO BE CONSIDERED EFFECTIVE

Meet all metrics designated in the "Consistently Implemented" level and half or greater of the metrics designated in the "Managed and Measurable" level.

Level 5 Optimized

Meet all metrics designated in the "Managed and Measurable" and "Optimized" levels.

Source: EPA OIG graphic.

Except for Ad Hoc and Optimized, which are the lowest and highest maturity levels, respectively, to achieve a maturity level, the agency must meet all metrics in prior level(s) and at least half of the metrics in the current level.

According to the FY 2016 Inspector General FISMA reporting metrics:

> "…Level 4, *Managed and Measurable*, represents an effective information security program.… Agencies with programs that score at or above the Managed and Measureable [level] for a NIST [National Institute of Standards and Technology] [Cybersecurity] Framework Function have "effective" programs within that area in accordance with the effectiveness definition in NIST SP 800-53, Rev. 4...."

Thus, CSB would have to have met all of the Consistently Implemented (level 3), Defined (level 2) and Ad-Hoc (levels 1) metrics, and half or greater of the Managed and Measurable (level 4) metrics, to be considered effective.

The CSB's principal role is to investigate chemical accidents 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 located in a federal center complex in Denver, Colorado. The CSB's staff includes investigators, engineers, safety experts, attorneys and administrators.

CSB investigated an industrial explosion and fire incident. (CSB photo)

Responsible Offices

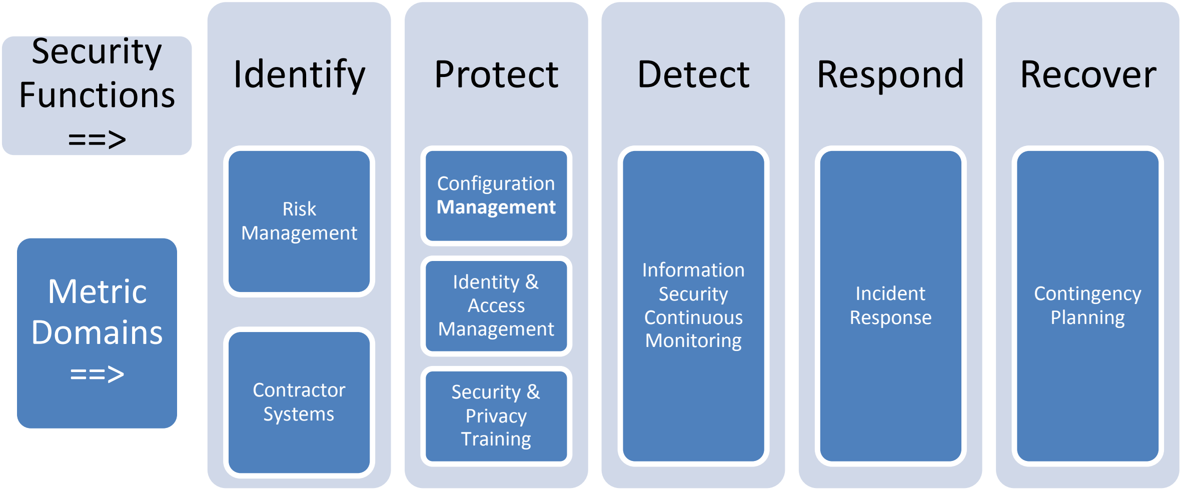
The CSB's Board Chairperson is responsible for agency administration. The CSB's Office of Administration is responsible for the information technology security program. The Chief Information Officer is responsible for making risk management decisions regarding deficiencies; their potential impact on 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 August 2016 to November 2016 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 based on the audit objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objectives.

We used the control self-assessment[1] methodology to assess the five Cybersecurity Framework Security Functions and corresponding metric domains as specified in the FY 2016 Inspector General FISMA reporting metrics version 1.1.3.

Figure 2: Cybersecurity framework security functions and corresponding Inspector General FISMA reporting metric domains



Source: EPA OIG graphic.

The control self-assessment of the CSB's information security program included collecting the CSB's control self-assessment responses to the FY 2016 Inspector General FISMA metrics; discussing the CSB's self-assessment with the Chief Information Officer; obtaining supporting evidence for the CSB's positive responses to the FISMA metrics to determine the veracity of CSB's responses; and collecting CSB management's feedback on our analysis, either verbally or through email. We performed limited testing of the Security and Privacy Training metric area to verify the ability to rely on CSB's self-assessment. We also followed up on the CSB's implementation status of prior report audit recommendations.

We believe using the control self-assessment methodology provides a reasonable basis for our conclusions and the information presented in this report.

We believe that the risk that CSB's information security continuous monitoring program has changed since the prior review is low because CSB has not made any material changes to its program since the last review in January 2016 and we conducted steps to validate that conclusions drawn in the last review are still valid. As a result, and due to time and resource constraints, we did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring

[1] According to the Institute of Internal Auditors, control self-assessment is a technique that allows personnel directly involved in the business process to participate in assessing the organization's risk management and control processes. Audit teams can use control self-assessment results to gather relevant information about risk and controls.

program. Similarly, due to time and resource constrains, we did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

Prior Reports

Since the beginning of FY 2015, we issued the following reports, which included recommendations, regarding CSB's information security program:

- **Report No. 16-P-0035, *CSB Needs Better Security Controls to Protect Critical Data Stored on Its Regional Servers*, dated November 5, 2015.** We reported that CSB should strengthen physical and environmental protection controls for its Western Regional Office server room. We also reported that CSB should take steps to implement the remaining four recommendations from our prior audit report to resolve security deficiencies cited. We made seven recommendations to CSB for improving its information security program. CSB agreed with these recommendations, took steps to complete one of the recommendations, and provided milestone dates for when it would complete the corrective actions for the remaining six recommendations. Based on our audit follow-up during this audit, CSB completed the agreed-to corrective actions that addressed the remaining six open recommendations. Therefore, we consider these recommendations closed (Recommendations 1, 2, 3, 4, 6 and 7).

- **Report No. 15-P-0073, *Key Aspects of CSB Information Security Program Need Improvement,* dated February 3, 2015.** We reported that CSB should improve key aspects of its information security program to better manage practices related to information security planning, physical and environmental security controls for its headquarters server room, its vulnerability testing process, and internal controls over the agency's information technology inventory. We made 17 recommendations to CSB to improve its information security program. Our subsequent follow-up during FY 2015 disclosed that CSB successfully completed 13 of the 17 recommendations. Our audit follow-up during this audit disclosed that CSB performed the agreed-to corrective actions that addressed the remaining four open recommendations. Therefore, we consider these recommendations closed (Recommendations 1, 2, 4 and 6).

Results of Review

We relied upon management's assertions in the CSB's control self-assessment responses to the FY 2016 Inspector General FISMA reporting metrics and supporting evidence provided for the CSB's positive responses.

We worked closely with CSB and briefed them on the audit results for each FISMA metric, and, where appropriate, we updated our analysis based on these discussions. CSB agreed with our results.

CSB is considered effective in two of the five information security function areas specified by the FY 2016 Inspector General FISMA reporting metrics, as shown in Table 1. The CyberScope system awards a maximum of 20 points per security function area. An area must score at least 18 points (at or above the Level 4 - Managed and Measurable maturity level) to be considered effective.

Table 1: Maturity level of CSB's information security function areas

Security function	Maturity level	Points achieved by function area	Minimum points needed to be considered effective
1. Identify	Level 5: Optimized	20	18
2. Protect	Level 3: Consistently Implemented	13	18
3. Detect	Level 3: Consistently Implemented	13	18
4. Respond	Level 2: Defined	7	18
5. Recover	Level 5: Optimized	20	18

Source: CyberScope scoring of FY 2016 metric results.

Several areas within the CSB's information security program were identified as receiving a Not Met response, which affected the agency's rating and ability to achieve Level 4 of the maturity model. Based on our analysis of CSB's control self-assessment, improvements are needed in the following security functions and corresponding metric domains:

- **Protect Security Function:**
  - **Identity and Access Management:** CSB has not fully implemented the use of Personal Identity Verification cards for physical and logical access.
  - **Security and Privacy Training:** CSB has not identified and tracked the specialized training requirements for users with significant information security and privacy responsibilities, and has not measured the effectiveness of its security and privacy awareness and training programs through the use of social engineering and phishing exercises.

- **Respond Security Function:**
  - **Incident Response:** CSB has not identified and fully defined the incident response technologies it plans to use.

Appendix A provides the responses for each FISMA metric section.

Appendix A

Department of Homeland Security CyberScope Template

Inspector General

Section Report

2016

Annual FISMA Report

Chemical Safety Board

Section 0: Overall

0.1 Please provide an overall narrative assessment of the agency's information security program. 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 this response to conform with the grammatical and narrative structure of the Annual Report.

CSB's information security program scored 73 out of the possible 100 points. Five Cybersecurity Framework Security Function areas and the corresponding metric domains listed below were assessed as specified by the fiscal year 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.

1. Identify
- **Risk Management**
- **Contractor Systems**

2. Protect
- **Configuration Management**
- **Identity and Access Management**
- **Security and Privacy Training**

3. Detect
- **Information Security Continuous Monitoring**

4. Respond
- **Incident Response**

5. Recover
- **Contingency Planning**

Each function area was assigned a maturity level rating of Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, or Optimized.

CSB's Identify and Recover function areas were rated as "Optimized." CSB's Protect and Detect function areas were rated as "Consistently Implemented." CSB's Respond function area was rated as "Defined." Improvements are needed within the Identify and Access Management, Security and Privacy Training, and Incident Response metric domains.

Section 1: Identify

Risk Management (Identify)

1.1 Has the organization established a risk management program that includes comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**

Met

1.1.1 Identifies and maintains an up-to-date system inventory, including organization- and contractor-operated systems, hosting environments, and systems residing in the public, hybrid, or private cloud. (2016 CIO FISMA Metrics, 1.1; NIST Cybersecurity Framework (CF) ID.AM.1, NIST 800-53: PM-5) **Defined**

Met

1.1.2 Develops a risk management function that is demonstrated through the development, implementation, and maintenance of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39) **Consistently Implemented**

Met

1.1.3 Incorporates mission and business process-related risks into risk-based decisions at the organizational perspective, as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39) **Consistently Implemented**

Met

1.1.4 Conducts information system level risk assessments that integrate risk decisions from the organizational and mission/business process perspectives and take into account threats, vulnerabilities, likelihood, impact, and risks from external parties and common control providers. (NIST SP 800-37, Rev. 1, NIST SP 800-39, NIST SP 800-53: RA-3) **Consistently Implemented**

Met

1.1.5 Provides timely communication of specific risks at the information system, mission/business, and organization-level to appropriate levels of the organization. **Managed and Measureable**

Met

1.1.6 Performs comprehensive assessments to categorize information systems in accordance with Federal standards and applicable guidance. (FIPS 199, FIPS 200, FISMA, Cybersecurity Sprint, OMB M-16-04, President's Management Council (PMC) cybersecurity assessments) **Consistently Implemented**

Met

1.1.7 Selects an appropriately tailored set of baseline security controls based on mission/business requirements and policies and develops procedures to employ controls within the information system and its environment of operation. **Defined**

Met

1.1.8 Implements the tailored set of baseline security controls as described in 1.1.7. **Consistently Implemented**

Met

1.1.9 Identifies and manages risks with system interconnections, including through authorizing system interconnections, documenting interface characteristics and security requirements, and maintaining interconnection security agreements. (NIST SP 800-53: CA-3) **Managed and Measureable**

Met

1.1.10 Continuously assesses the security controls, including hybrid and shared controls, using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. **Consistently Implemented**

Met

1.1.11 Maintains ongoing information system authorizations based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable (OMB M-14-03, NIST Supplemental Guidance on Ongoing Authorization). **Managed and Measureable**

Met

1.1.12 Security authorization package contains system security plan, security assessment report, and POA&M that are prepared and maintained in accordance with government policies. (SP 800-18, SP 800-37) **Managed and Measureable**

Met

1.1.13 POA&Ms are maintained and reviewed to ensure they are effective for correcting security weaknesses. **Consistently Implemented**

Met

1.1.14 Centrally tracks, maintains, and independently reviews/validates POA&M activities at least quarterly. (NIST SP 800-53 :CA-5; OMB M-04-25) **Managed and Measureable**

Met

1.1.15 Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks. **Managed and Measureable**

Met

Section 1: Identify

1.1.16 Implemented an insider threat detection and prevention program, including the development of comprehensive policies, procedures, guidance, and governance structures, in accordance with Executive Order 13587 and the National Insider Threat Policy. (PMC; NIST SP 800-53: PM-12)

Consistently Implemented

Met

Comments: The Chief Information Officer indicated that CSB has no classified networks or classified information.

1.1.17 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. Based on all testing performed, is the Risk Management program effective?

Effective

Comments: We did not assess this question.

Contractor Systems (Identify)

1.2 Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including other government agencies, managed hosting environments, and systems and services residing in a cloud external to the organization that is inclusive of policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Defined

Met

1.2.1 Establishes and implements a process to ensure that contracts/statements of work/solicitations for systems and services, include appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information. (FAR Case 2007-004, Common Security Configurations, FAR Sections 24.104, 39.101, 39.105, 39.106, 52.239-1; PMC, 2016 CIO Metrics 1.8, NIST 800-53, SA-4 FedRAMP standard contract clauses; Cloud Computing Contract Best Practices)

Consistently Implemented

Met

1.2.2 Specifies within appropriate agreements how information security performance is measured, reported, and monitored on contractor- or other entity-operated systems. (CIO and CAO Council Best Practices Guide for Acquiring IT as a Service, NIST SP 800-35)

Consistently Implemented

Met

1.2.3 Obtains sufficient assurance that the security controls of systems operated on the organization's behalf by contractors or other entities and services provided on the organization's behalf meet FISMA requirements, OMB policy, and applicable NIST guidelines. (NIST SP 800-53: CA-2, SA-9)

Consistently Implemented

Met

1.2.4 Provide any additional information on the effectiveness (positive or negative) of the organization’s Contractor Systems Program that was not noted in the questions above. Based on all testing performed, is the Contractor Systems Program effective?

Effective

Comments: We did not assess this question.

Level	Score	Possible Score
LEVEL 5: Optimized	20	20

Section 2: Protect

Configuration Management (Protect)

2.1 Has the organization established a configuration management program that is inclusive of comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**

Met

2.1.1 Develops and maintains an up-to-date inventory of the hardware assets (i.e., endpoints, mobile assets, network devices, input/output assets, and SMART/NEST devices) connected to the organization's network with the detailed information necessary for tracking and reporting. (NIST CF ID.AM-1; 2016 CIO FISMA Metrics 1.5, 3.17; NIST 800-53: CM-8) **Defined**

Met

2.1.2 Develops and maintains an up-to-date inventory of software platforms and applications used within the organization and with the detailed information necessary for tracking and reporting. (NIST 800-53: CM-8, NIST CF ID.AM-2) **Defined**

Met

2.1.3 Implements baseline configurations for IT systems that are developed and maintained in accordance with documented procedures. (NIST SP 800-53: CM-2; NIST CF PR.IP-1) **Consistently Implemented**

Met

2.1.4 Implements and maintains standard security settings (also referred to as security configuration checklists or hardening guides) for IT systems in accordance with documented procedures. (NIST SP 800-53: CM-6; CIO 2016 FISMA Metrics, 2.3) **Consistently Implemented**

Met

2.1.5 Assesses configuration change control processes, including processes to manage configuration deviations across the enterprise that are implemented and maintained. (NIST SP 800-53: CM-3, NIST CF PR.IP-3) **Managed and Measureable**

Met

2.1.6 Identifies and documents deviations from configuration settings. Acceptable deviations are approved with business justification and risk acceptance. Where appropriate, automated means that enforce and redeploy configuration settings to systems at regularly scheduled intervals are deployed, while evidence of deviations is also maintained. (NIST SP 800-53: CM-6, Center for Internet Security Controls (CIS) 3.7) **Managed and Measureable**

Met

2.1.7 Implemented SCAP certified software assessing (scanning) capabilities against all systems on the network to assess both code-based and configuration-based vulnerabilities in accordance with risk management decisions. (NIST SP 800-53: RA-5, SI- 2; CIO 2016 FISMA Metrics 2.2, CIS 4.1) **Managed and Measureable**

Met

2.1.8 Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2) **Consistently Implemented**

Met

2.1.9 Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01) **Managed and Measureable**

Met

2.1.10 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. Based on all testing performed, is the Configuration Management Program effective?

Effective

Comments: We did not assess this question.

Identity and Access Management (Protect)

2.2 Has the organization established an identity and access management program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**

Met

2.2.1 Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements, participate in required training prior to being granted access, and recertify access agreements on a predetermined interval. (NIST 800-53: PL-4, PS-6) **Consistently Implemented**

Met

2.2.2 Ensures that all users are only granted access based on least privilege and separation-of-duties principles. **Consistently Implemented**

Met

Comments: CSB has documented processes for this area; however, CSB did not provide support that these processes were implemented.

2.2.3 Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. networking devices, such as load balancers and intrusion detection/prevention systems, and other input/output devices **Consistently Implemented** such as faxes and IP phones).

Met

Comments: CSB stated that they inventory hardware assets with a cost of $500 or more. Additionally, they stated that all such hardware assets at the CSB (desktops, laptops, servers, network devices, switches) do have user accounts.

2.2.4 Implements PIV for physical access in accordance with government policies. (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11)

Consistently Implemented

Not Met

Comments: CSB currently uses Personal Identity Verification cards for access to the server room in Headquarters and will use the same process in the Western Regional Office server room as soon as General Service Administration installs a card reader in that location.

2.2.5 Implements PIV or a NIST Level of Assurance (LOA) 4 credential for logical access by all privileged users (system, network, database administrators, and others responsible for system/application control, monitoring, or administration functions). (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.5.1)

Consistently Implemented

Not Met

Comments: Implementation of two-factor authentication with Entrust is in progress.

2.2.6 Enforces PIV or a NIST LOA 4 credential for logical access for at least 85% of non-privileged users. (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.4.1)

Consistently Implemented

Not Met

Comments: Implementation of two-factor authentication with Entrust is in progress.

2.2.7 Tracks and controls the use of administrative privileges and ensures that these privileges are periodically reviewed and adjusted in accordance with organizationally defined timeframes. (2016 CIO FISMA Metrics 2.9, 2.10; OMB M-16-04, CIS 5.2)

Managed and Measureable

Met

Comments: CSB has documented processes for this area; however, CSB did not provide support that these processes were implemented.

2.2.8 Ensures that accounts are terminated or deactivated once access is no longer required or after a period of inactivity, according to organizational policy.

Managed and Measureable

Met

Comments: CSB has documented processes for this area; however, CSB did not provide support that these processes were implemented.

2.2.9 Identifies, limits, and controls the use of shared accounts. (NIST SP 800-53: AC-2) **Consistently Implemented**

Met

Comments: CSB has documented processes for this area; however, CSB did not provide support that these processes were implemented.

2.2.10 All users are uniquely identified and authenticated for remote access using Strong Authentication (multi-factor), including PIV. (NIST SP 800-46, Section 4.2, Section 5.1, NIST SP 800-63) **Consistently Implemented**

Not Met

Comments: Implementation of two-factor authentication with Entrust is in progress.

2.2.11 Protects against and detects unauthorized remote access connections or subversion of authorized remote access connections, including through remote scanning of host devices. (CIS 12.7, 12.8, FY 2016 CIO FISMA metrics 2.17.3, 2.17.4, 3.11, 3.11.1) **Consistently Implemented**

Met

2.2.12 Remote access sessions are timed-out after 30 minutes of inactivity, requiring user re-authentication, consistent with OMB M-07-16 **Managed and Measureable**

Met

2.2.13 Enforces a limit of consecutive invalid remote access logon attempts and automatically locks the account or delays the next logon prompt. (NIST 800-53: AC-7) **Consistently Implemented**

Met

2.2.14 Implements a risk-based approach to ensure that all agency public websites and services are accessible through a secure connection through the use and enforcement of https and strict transport security. (OMB M-15-13) **Consistently Implemented**

Met

2.2.15 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. Based on all testing performed is the Identity and Access Management Program effective?

Effective

Comments: We did not assess this question.

Security and Privacy Training (Protect)

2.3 Has the organization established a security and privacy awareness and training program, including comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**

Met

2.3.1 Develops training material for security and privacy awareness training containing appropriate content for the organization, including anti-phishing, malware defense, social engineering, and insider threat topics. (NIST SP 800-50, 800-53: AR-5, OMB M-15-01, 2016 CIO Metrics, PMC, National Insider Threat Policy (NITP)) **Consistently Implemented**

Met

2.3.2 Evaluates the skills of individuals with significant security and privacy responsibilities and provides additional security and privacy training content or implements human capital strategies to close identified gaps. (NIST SP 800-50) **Consistently Implemented**

Met

2.3.3 Identifies and tracks status of security and privacy awareness training for all information system users (including employees, contractors, and other organization users) requiring security awareness training with appropriate internal processes to detect and correct deficiencies. (NIST 800-53: AT-2) **Consistently Implemented**

Met

2.3.4 Identifies and tracks status of specialized security and privacy training for all personnel (including employees, contractors, and other organization users) with significant information security and privacy responsibilities requiring specialized training. **Consistently Implemented**

Not Met

Comments: CSB stated that due to budget and scheduling priorities, the CSB did not have specialized IT security training in FY 2016. CSB also stated that they do, however, have such training paid for and being scheduled for FY 2017 at Learning Tree, and some of this training will be completed by the end of calendar year 2016. Additionally, CSB stated that they are also in the process of registering IT staff for the Department of Homeland Security's Cyber Security Virtual Learning Center and will begin taking courses in calendar year 2016.

2.3.5 Measures the effectiveness of its security and privacy awareness and training programs, including through social engineering and phishing exercises. (PMC, 2016 CIO FISMA Metrics 2.19, NIST SP 800-50, NIST SP 800-55) **Managed and Measureable**

Not Met

Comments: Per the Chief Information Officer, CSB has not conducted social engineering or phishing exercises in house.

2.3.6 Provide any additional information on the effectiveness (positive or negative) of the organization's Security and Privacy Training Program that was not noted in the questions above. Based on all testing performed is the Security and Privacy Training Program effective?

Effective

Comments: We did not assess this question.

Level	Score	Possible Score
LEVEL 3: Consistently Implemented	13	20

Section 3: Detect

Level 1

Definition

3.1.1 ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.

People

3.1.1.1 ISCM stakeholders and their responsibilities have not been fully defined and communicated across the organization. **Ad Hoc**

Met

3.1.1.2 The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Key personnel do not possess knowledge, skills, and abilities to successfully implement an effective ISCM program. **Ad Hoc**

Met

3.1.1.3 The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions. **Ad Hoc**

Met

3.1.1.4 The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. **Ad Hoc**

Met

Processes

3.1.1.5 ISCM processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. **Ad Hoc**

Met

3.1.1.6 ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **Ad Hoc**

Met

3.1.1.7 The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. **Ad Hoc**

Met

3.1.1.8 The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes. **Ad Hoc**

Met

Technology

3.1.1.9 The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. Use of ISCM technologies in the following areas is ad-hoc. **Ad Hoc**

- Patch management
- License management
- Information management
- Software assurance
- Vulnerability management
- Event management
- Malware detection
- Asset management
- Configuration management
- Network management
- Incident management

Met

3.1.1.10 The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Ad Hoc**

Met

Level 2

Definition

3.2.1 The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide.

People

3.2.1.1 ISCM stakeholders and their responsibilities have been defined and communicated across the organization. However, stakeholders **Defined** may not have adequate resources (people, processes, and technology) to effectively implement ISCM activities.

Met

3.2.1.2 The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective ISCM program.

Defined

Met

3.2.1.3 The organization has defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. However, ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions.

Defined

Met

3.2.1.4 The organization has defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. However, ISCM activities are not consistently integrated with the organization's risk management program.

Defined

Met

Processes

3.2.1.5 ISCM processes have been fully defined for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. However, these processes are inconsistently implemented across the organization.

Defined

Met

3.2.1.6 ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used.

Defined

Met

3.2.1.7 The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization.

Defined

Met

3.2.1.8 The organization has a defined process for capturing lessons learned on the effectiveness of its ISCM program and making necessary improvements. However, lessons learned are not consistently shared across the organization and used to make timely improvements

Defined

to the ISCM program.

Met

Technology

3.2.1.9 The organization has identified and fully defined the ISCM technologies it plans to utilize in the following automation areas. In addition, the organization has developed a plan for implementing ISCM technologies in these areas: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. However, the organization has not fully implemented technology is these automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some ISCM activities, the tools may not be interoperable. **Defined**

Met

3.2.1.10 The organization has defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. However, the organization does not consistently implement the technologies that will enable it to manage an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Defined**

Met

Level 3

Definition

3.3.1 In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions, consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.

People

3.3.1.1 ISCM stakeholders and their responsibilities have been identified and communicated across the organization, and stakeholders have adequate resources (people, processes, and technology) to effectively implement ISCM activities. **Consistently Implemented**

Met

3.3.1.2 The organization has fully implemented its plans to close any gapes in skills, knowledge, and resources required to successfully implement an ISCM program. Personnel possess the required knowledge, skills, and abilities to effectively implement the organization's ISCM program. **Consistently Implemented**

Section 3: Detect

Met

3.3.1.3 ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations. **Consistently Implemented**

Met

3.3.1.4 ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements. **Consistently Implemented**

Met

Processes

3.3.1.5 ISCM processes are consistently performed across the organization in the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. **Consistently Implemented**

Met

3.3.1.6 The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. **Consistently Implemented**

Met

3.3.1.7 The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting. ISCM measures provide information on the effectiveness of ISCM processes and activities. **Consistently Implemented**

Met

3.3.1.8 The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes. **Consistently Implemented**

Met

3.3.1.9 The organization has consistently implemented its defined technologies in all of the following ISCM automation areas. ISCM tools are interoperable to the extent practicable. **Consistently Implemented**

- Patch management
- License management
- Information management
- Software assurance

- Vulnerability management
- Event management
- Malware detection
- Asset management
- Configuration management
- Network management
- Incident management

Met

Technology

3.3.1.10 The organization can produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Consistently Implemented**

Met

Level 4

Definition

3.4.1 In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.

People

3.4.1.1 The organization's staff is consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of the organization's ISCM program. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

3.4.1.2 Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the ISCM program. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

3.4.1.3 Staff are assigned responsibilities for developing and monitoring ISCM metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the ISCM program. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

Processes

3.4.1.4 The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing ISCM. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

3.4.1.5 Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

3.4.1.6 The organization is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

3.4.1.7 The organization uses its ISCM metrics for determining risk response actions including risk acceptance, avoidance/rejection, or transfer. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

3.4.1.8 ISCM metrics are reported to the organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

3.4.1.9 ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, **Managed and Measureable**

Security Assessment Report, and POA&M) up to date on an ongoing basis.

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

Technology

3.4.1.10 The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing ISCM. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

3.4.1.11 The organization's ISCM performance measures include data on the implementation of its ISCM program for all sections of the network from the implementation of technologies that provide standard calculations, comparisons, and presentations. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

3.4.1.12 The organization utilizes a SIEM tool to collect, maintain, monitor, and analyze IT security information, achieve situational awareness, and manage risk **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

Level 5

Definition

3.5.1 In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.

People

3.5.1.1 The organization's assigned personnel collectively possess a high skill level to perform and update ISCM activities on a near real-time basis to make any changes needed to address ISCM results based on organization risk tolerance, the threat environment, and business/mission requirements. **Optimized**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

Section 3: Detect

Processes

3.5.1.2 The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity and practices. **Optimized**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

3.5.1.3 On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. **Optimized**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

3.5.1.4 The ISCM program is fully integrated with strategic planning, enterprise architecture and capital planning and investment control processes, and other mission/business areas, as appropriate. **Optimized**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

3.5.1.5 The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact. **Optimized**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

Technology

3.5.1.6 The organization has institutionalized the implementation of advanced cybersecurity technologies in near real-time. **Optimized**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

3.5.1.7 The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its ISCM program. **Optimized**

Not Met

Comments: We did not assess maturity levels 4 and 5 of the CSB's Information Security Continuous Monitoring program.

Level	Score	Possible Score
LEVEL 3: Consistently Implemented	13	20

Section 4: Respond

Level 1

Definition

4.1.1 Incident response program is not formalized and incident response activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines).

People

4.1.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have not been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. **Ad Hoc**

Met

4.1.1.2 The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. Key personnel do not possess the knowledge, skills, and abilities to successfully implement an effective incident response program. **Ad Hoc**

Met

4.1.1.3 The organization has not defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. **Ad Hoc**

Met

4.1.1.4 The organization has not defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Ad Hoc**

Met

Processes

4.1.1.5 Incident response processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting to internal and external stakeholders using standard data elements and impact classifications within timeframes established by US-CERT. **Ad Hoc**

Met

4.1.1.6 The organization has not fully defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical **Ad Hoc** assistance/surge resources/special capabilities for quickly responding to incidents.

Met

4.1.1.7 The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. **Ad Hoc**

Met

4.1.1.8 The organization has not defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. **Ad Hoc**

Met

Technology

4.1.1.9 The organization has not identified and defined the incident response technologies needed in one or more of the following areas and relies on manual/procedural methods in instances where automation would be more effective. Use of incident response technologies in the following areas is ad-hoc. **Ad Hoc**

- 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 anti-virus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools

Met

4.1.1.10 The organization has not defined how it will meet the defined Trusted Internet Connection (TIC) security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. **Ad Hoc**

Met

4.1.1.11 The organization has not defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks. **Ad Hoc**

Met

4.1.1.12 The organization has not defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. **Ad Hoc**

Met

Level 2

Section 4: Respond

Definition

4.2.1 The organizational has formalized its incident response program through the development of comprehensive incident response policies, plans, and procedures consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, incident response policies, plans, and procedures are not consistently implemented organization-wide.

People

4.2.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement incident response activities. Further, the organization has not verified roles and responsibilities as part of incident response testing. **Defined**

Met

4.2.1.2 The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective incident response program. **Defined**

Met

4.2.1.3 The organization has defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. However, the organization does not consistently utilize its threat vector taxonomy and incident response information is not always shared with individuals with significant security responsibilities and other stakeholders in a timely manner. **Defined**

Met

4.2.1.4 The organization has defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. However, incident response activities are not consistently integrated with these areas. **Defined**

Met

Processes

4.2.1.5 Incident response processes have been fully defined for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, **Defined** and reporting using standard data elements and impact classifications within timeframes established by US-CERT. However, these processes are inconsistently implemented across the organization.

Met

4.2.1.6 The organization has fully defined, but not consistently implemented, its processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. **Defined**

Met

4.2.1.7 The organization has identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. **Defined**

Met

4.2.1.8 The organization has defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. However, lessons learned are not consistently captured and shared across the organization and used to make timely improvements to security controls and the incident response program. **Defined**

Met

Technology

4.2.1.9 The organization has identified and fully defined the incident response technologies it plans to utilize in the following areas: **Defined**

- 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. However, the organization has not ensured that security and event data are aggregated and correlated from all relevant sources and sensors.
- Malware detection such as Anti-virus and antispam software technologies
- Information management such as data loss prevention
- File integrity and endpoint and server security tools

However, the organization has not fully implemented technologies in these areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization’s network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization’s incident response policy, plans, and procedures.

Not Met

Section 4: Respond

Comments: CSB has not defined the incident response technologies needed for the areas described in this metric.

4.2.1.10 The organization has defined how it will meet the defined TIC security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. However, the organization has not ensured that the TIC 2.0 provider and agency managed capabilities are consistently implemented. **Defined**

Met

4.2.1.11 The organization has defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its networks. **Defined**

Met

4.2.1.12 The organization has defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. However, the organization has not established, and does not consistently maintain, a comprehensive baseline of network operations and expected data flows for users and systems. **Defined**

Met

Level 3

Definition

4.3.1 In addition to the formalization and definition of its incident response program (Level 2), the organization consistently implements its incident response program across the agency, in accordance with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, data supporting metrics on the effectiveness of the incident response program across the organization are not verified, analyzed, and correlated.

People

4.3.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined, communicated, and consistently implemented across the organization (Level 2). Further, the organization has verified roles and responsibilities of incident response stakeholders as part of incident response testing. **Consistently Implemented**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.3.1.2 The organization has fully implemented its plans to close any gaps in the skills, knowledge, and resources needed to effectively implement its incident response program. Incident response teams are periodically trained to ensure that knowledge, skills, and abilities are maintained. **Consistently Implemented**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.3.1.3 The organization consistently utilizes its defined threat vector taxonomy and shares information with individuals with significant security responsibilities and other stakeholders in a timely fashion to support risk-based decision making. **Consistently Implemented**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.3.1.4 Incident response activities are integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Consistently Implemented**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

Processes

4.3.1.5 Incident response processes are consistently implemented across the organization for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. **Consistently Implemented**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.3.1.6 The organization has ensured that processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents are implemented consistently across the organization. **Consistently Implemented**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.3.1.7 The organization is consistently capturing qualitative and quantitative performance metrics on the performance of its incident response program. However, the organization has not ensured that the data supporting the metrics was obtained accurately and in a reproducible format or that the data is analyzed and correlated in ways that are effective for risk management. **Consistently Implemented**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

Section 4: Respond

4.3.1.8 The organization is consistently collecting and capturing lessons learned and incident data on the effectiveness of its incident response program and activities. However, lessons learned may not be shared across the organization in a timely manner and used to make timely improvements to the incident response program and security measures. **Consistently Implemented**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.3.1.9 The rigor, intensity, scope, and results of incident response activities (i.e. preparation, detection, analysis, containment, eradication, and recovery, reporting and post incident) are comparable and predictable across the organization. **Consistently Implemented**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

Technology

4.3.1.10 The organization has consistently implemented its defined incident response technologies in the following areas: **Consistently Implemented**

- 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. The organization ensures that security and event data are aggregated and correlated from all relevant sources and sensors
- Malware detection, such as anti-virus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools

In addition, the tools are interoperable to the extent practicable, cover all components of the organization’s network, and have been configured to collect and retain relevant and meaningful data consistent with the organization’s incident response policy, procedures, and plans.

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.3.1.11 The organization has consistently implemented defined TIC security controls and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. **Consistently Implemented**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

Section 4: Respond

4.3.1.12 The organization is utilizing DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving their networks. **Consistently Implemented**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.3.1.13 The organization has fully implemented technologies to develop and maintain a baseline of network operations and expected data flows for users and systems. **Consistently Implemented**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

Level 4

Definition

4.4.1 In addition to being consistently implemented (Level 3), incident response activities are repeatable and metrics are used to measure and manage the implementation of the incident response program, achieve situational awareness, and control ongoing risk. In addition, the incident response program adapts to new requirements and government-wide priorities.

People

4.4.1.1 Incident response stakeholders are consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and are collecting, analyzing, and reporting data on the effectiveness of the organization's incident response program. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.4.1.2 Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the incident response program. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.4.1.3 Incident response stakeholders are assigned responsibilities for developing and monitoring incident response metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the incident response program. **Managed and Measureable**

Not Met

Section 4: Respond

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

Processes

4.4.1.4 The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing incident response. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.4.1.5 Data supporting incident response measures and metrics are obtained accurately, consistently, and in a reproducible format. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.4.1.6 Incident response data, measures, and metrics are analyzed, collected, and presented using standard calculations, comparisons, and presentations **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.4.1.7 Incident response metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

Technology

4.4.1.8 The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.4.1.9 The organization's incident response performance measures include data on the implementation of its incident response program for all sections of the network. **Managed and Measureable**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

Level 5

Definition

4.5.1 In addition to being managed and measurable (Level 4), the organization's incident response program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements, and a changing threat and technology landscape.

People

4.5.1.1 The organization's assigned personnel collectively possess a high skill level to perform and update incident response activities on a near real-time basis to make any changes needed to address incident response results based on organization risk tolerance, the threat environment, and business/mission requirements. **Optimized**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

Processes

4.5.1.2 The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity practices. **Optimized**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.5.1.3 On a near real-time basis, the organization actively adapts its incident response program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a near real-time manner. **Optimized**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.5.1.4 The incident response program is fully integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Optimized**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.5.1.5 The incident response program achieves cost-effective IT security objectives and goals and influences decision making that is based **Optimized** on cost, risk, and mission impact.

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

Technology

4.5.1.6 The organization has institutionalized the implementation of advanced incident response technologies in near real-time. **Optimized**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.5.1.7 The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its incident response program. **Optimized**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

4.5.1.8 The organization uses simulation based technologies to continuously determine the impact of potential security incidents to its IT assets and adjusts incident response processes and security measures accordingly. **Optimized**

Not Met

Comments: We did not assess maturity levels 3, 4 and 5 of the CSB's Incident Response program.

Level	Score	Possible Score
LEVEL 2: Defined	7	20

Section 5: Recover

Contingency Planning (Recover)

5.1 Has the organization established an enterprise-wide business continuity/disaster recovery program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**

Met

5.1.1 Develops and facilitates recovery testing, training, and exercise (TT&E) programs. (FCD1, NIST SP 800-34, NIST SP 800-53) **Consistently Implemented**

Met

5.1.2 Incorporates the system's Business Impact Analysis and Business Process Analysis into analysis and strategy toward development of the organization's Continuity of Operations Plan, Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). (NIST SP 800-34) **Consistently Implemented**

Met

5.1.3 Develops and maintains documented recovery strategies, plans, and procedures at the division, component, and IT infrastructure levels. (NIST SP 800-34) **Consistently Implemented**

Met

5.1.4 BCP and DRP are in place and ready to be executed upon if necessary. (FCD1, NIST SP 800-34, 2016 CIO FISMA Metrics 5.3, PMC) **Consistently Implemented**

Met

5.1.5 Tests BCP and DRP for effectiveness and updates plans as necessary. (2016 CIO FISMA Metrics, 5.4) **Managed and Measureable**

Met

5.1.6 Tests system-specific contingency plans, in accordance with organizationally defined timeframes, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4) **Consistently Implemented**

Met

5.1.7 Develops after-action reports that address issues identified during contingency/disaster recovery exercises in order to improve contingency/disaster recovery processes. (FCD1, NIST SP 800-34) **Managed and Measureable**

Met

5.1.8 Determines alternate processing and storage sites based upon risk assessments which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized, and are not subject to the same physical and/or **Consistently Implemented** cybersecurity risks as the primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-6, CP-7)

Met

5.1.9 Conducts backups of information at the user- and system-levels and protects the confidentiality, integrity, and availability of backup information at storage sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-9, NIST CF, PR.IP-4, NARA guidance on information systems security records) **Managed and Measureable**

Met

5.1.10 Contingency planning that considers supply chain threats. **Defined**

Met

5.1.11 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. Based on all testing performed is the Contingency Planning Program effective?

Effective

Comments: We did not assess this question.

Level	Score	Possible Score
LEVEL 5: Optimized	20	20

APPENDIX A: Maturity Model Scoring

Maturity Levels by Section

Section	Level	Score	Possible Score
Section 1: Identify	LEVEL 5: Optimized	20	20
Section 2: Protect	LEVEL 3: Consistently Implemented	13	20
Section 3: Detect	LEVEL 3: Consistently Implemented	13	20
Section 4: Respond	LEVEL 2: Defined	7	20
Section 5: Recover	LEVEL 5: Optimized	20	20
TOTAL		73	100

Section 1: Identify

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	4	0	4	100%	4	4
Consistently Implemented	11	0	11	100%	6	6
Managed and Measureable	6	0	6	100%	5	5
Optimized	0	0	0	100%	2	2
EFFECTIVE						

Section 2: Protect

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	5	0	5	100%	4	4
Consistently Implemented	13	5	18	72%	6	6
Managed and Measureable	7	1	8	88%	0	5
Optimized	0	0	0	100%	0	2

Section 3: Detect

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	10	0	10	100%	3	3
Defined	10	0	10	100%	4	4
Consistently Implemented	10	0	10	100%	6	6
Managed and Measureable	0	12	12	0%	0	5
Optimized	0	7	7	0%	0	2

Section 4: Respond

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	12	0	12	100%	3	3
Defined	11	1	12	92%	4	4
Consistently Implemented	0	13	13	0%	0	6
Managed and Measureable	0	9	9	0%	0	5
Optimized	0	8	8	0%	0	2

Section 5: Recover

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	2	0	2	100%	4	4
Consistently Implemented	6	0	6	100%	6	6
Managed and Measureable	3	0	3	100%	5	5
Optimized	0	0	0	100%	2	2
EFFECTIVE						

Distribution

Chairperson and Board 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
Deputy Director of Administration, U.S. Chemical Safety and Hazard Investigation Board