U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

U.S. Chemical Safety Board

Fiscal Year 2015 Federal Information Security Modernization Act Report: Status of CSB's Information Security Program

Report No. 16-P-0086 **January 27, 2016**

Report Contributors:

Rudolph M. Brevard
Charles M. Dade
Nancy Dao
Nii-Lantei Lamptey
Christina Nelson

Abbreviations

CSB	U.S. Chemical Safety and Hazard Investigation Board
DHS	U.S. Department of Homeland Security
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification

Cover photo: A PIV card, used for logical access, being inserted into a laptop card reader. (EPA OIG photo)

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

16-P-0086
January 27, 2016

At a Glance

Why We Did This Review

The Office of Inspector General performed this audit to conduct a baseline assessment of the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) implementation of the information security policies and practices outlined by the 2015 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) reporting metrics.

FISMA requires federal agencies to develop an information security program that protects the operations and assets of the agency. The OIG performs an annual independent evaluation of the 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.

Fiscal Year 2015 Federal Information Security Modernization Act Report: Status of CSB's Information Security Program

What We Found

The effectiveness of the CSB's information security program is challenged by its lack of personal identity verification cards for logical access, complete system inventory, and documented policies and procedures for specialized security training.

We determined the CSB's baseline assessment of its information security areas using the criteria specified by the fiscal year 2015 Department of Homeland Security FISMA reporting metrics. This included collecting evidence of the existence of the CSB's policies and procedures, the CSB's self-assessment responses to the fiscal year 2015 FISMA metrics, and a discussion of CSB's control self-assessment with CSB management of selected information system security controls designated by the FISMA metrics. According to our control self-assessment results, the CSB information security program fully met the following FISMA metric sections:

- Continuous Monitoring Management.
- Configuration Management.
- Incident Response and Reporting.
- Risk Management.
- Plan of Action and Milestones.
- Remote Access Management.
- Contingency Planning.

For the remaining metrics, management attention is needed to improve processes that potentially could place these areas at risk.

- **Identity and Access Management.** CSB has not implemented the use of personal identification verification cards for logical access into its systems.
- **Security Training.** CSB does not have policies or procedures that specify the specialized training requirements for users with significant information security responsibilities.
- **Contractor Systems.** CSB lacks an inventory of systems operated on behalf of the agency, and does not have assurance that the security controls for those systems are effectively implemented.

Appendix A contains the U.S. Department of Homeland Security reporting metrics on the results of our analysis. CSB agreed with our results, and its complete response is in Appendix B.

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

THE INSPECTOR GENERAL

January 27, 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 baseline assessment of the U.S. Chemical Safety and Hazard Investigation Board's implementation of the information security policies and practices outlined by the 2015 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 conduct a baseline assessment of the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) implementation of the information system security policies and procedures, as outlined by the U.S. Department of Homeland Security's (DHS's) fiscal year (FY) 2015 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) reporting metrics.

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.

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 Region Office is located in a federal center complex in Denver, Colorado. The CSB's staff includes investigators, engineers, safety experts, attorneys and administrators.

CSB personnel assess damage at an accident site. (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 and Deputy Chief Information Officer are 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 November 2015 to January 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. Due to time constraints and the broad scope of the FISMA reporting metrics, the audit team did not test the implementation or the effectiveness of the established guidance or the operational effectiveness of the CSB's information security program. In these instances, we relied upon management's assertions as provided in response to our control self-assessment questionnaire. We believe using the control self-assessment[1] methodology provides a reasonable basis for our conclusions and the information presented in this report.

We received the Office of Management and Budget's (OMB's) FY 2015 FISMA reporting instructions on October 30, 2015. These instructions required small agencies to meet the same FISMA reporting requirements as larger federal agencies. Due to this significant change in FISMA reporting from prior years, we met with OMB to establish the due date of January 31, 2016, for us to submit this report to OMB.

Our audit of the CSB's information security program baseline assessment was limited to collecting evidence of the existence of the CSB's policies and procedures, the CSB's self-assessment responses to the FY 2015 FISMA reporting metrics, and a control self-assessment walkthrough with CSB management of selected information system security controls designated by the FISMA metrics.

We collected management's feedback on the analysis either verbally or through email. We worked closely with CSB and briefed them on the audit results for each portion of the FISMA metrics. Where appropriate, we updated our analysis based on our discussions.

Prior Reports

Since the beginning of FY 2015, we issued the following reports 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

[1] 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 utilize control self-assessment results to gather relevant information about risk and controls.

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. We consider these recommendations open with corrective actions pending.

- **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. CSB plans to complete the corrective actions for the four remaining recommendations by January 30, 2016.

Results of Review

We used a control self-assessment methodology to determine the CSB's baseline assessment of its information security areas using the criteria specified within the FY 2015 FISMA metrics. Our analysis of the control self-assessment results disclosed that the CSB's information security program fully met the following FISMA metric sections:

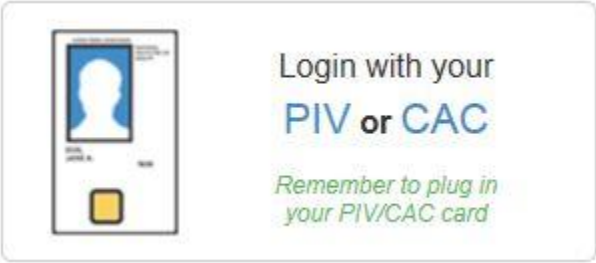
- Continuous Monitoring Management.
- Configuration Management.
- Incident Response and Reporting.
- Risk Management.
- Plan of Action and Milestones.
- Remote Access Management.
- Contingency Planning.

Appendix A provides a detailed analysis and responses for each FISMA metric section.

CSB complied with selected criteria within its Identity and Access Management, Security Training, and Contractor Systems FISMA programs. However, due to negative responses to certain FISMA metric attributes and our walkthrough of CSB's control processes, process improvements are needed in the following metrics:

- **Security Training:** CSB does not have policies and procedures that specify the specialized training requirements for users with significant information security responsibilities.

- **Contractor Systems**: CSB does not have a complete inventory of systems operated on the organization's behalf, the inventory is not updated annually, and the agency does not have sufficient assurance that security controls of contractor systems are effectively implemented and compliant with federal requirements.
- **Identity and Access Management:** CSB has not implemented the use of personal identification verification (PIV)[2] cards for logical access into its systems.



Example of a required PIV card login.
(MAX.gov login image)

Conclusion

While CSB has implemented a security program consistent with the majority of the selected FISMA criteria, the agency needs process improvements within the Identity and Access Management, Security Training, and Contractor Systems FISMA programs. As such, questions exist as to whether CSB is doing all it can to protect the confidentiality, integrity and availability of information technology resources and stored data.

CSB Response and OIG Evaluation

CSB's response to our discussion draft report is in Appendix B. CSB agreed overall with our audit results. CSB indicated it has planned for, but has not implemented, logical access to its systems with PIV credentials. CSB stated its laptops and desktops all have PIV readers or the capability to use external PIV readers. However, CSB stated it is still evaluating the risks of using PIV credentials for logical access, especially for investigators and other users in the field. Upon further discussions with CSB, we discovered that CSB is in the

[2] A PIV card is a smart card issued to an individual that contains a PIV Card Application which stores identity credentials so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

planning phase for implementing PIV card access to its systems, but has not yet developed a formal plan of action.

CSB indicated that Individual Development Plans are reviewed annually for users with significant information security responsibilities that include specific training requirements in specialized job-related functions. CSB stated it has also developed a draft order related to Individual Development Planning for not only information technology personnel but for all its employees, to ensure they acquire the necessary specialized training. CSB stated it will evaluate additional language in an update to its order on information security (Board Order 34) to include language that stipulates specialized training for users with significant information security responsibilities.

CSB indicated it receives financial and human resources services from other agencies in the federal government and had not included these systems in its System Security Plan. CSB stated it will work to add these systems to the updated System Security Plan and acquire the necessary supporting documentation regarding the servicing agency's implementation of security controls.

We agree with CSB's response and will conduct follow-up work to assess CSB's progress during the FY 2016 FISMA audit.

Appendix A

Department of Homeland Security CyberScope Template

Inspector General

Section Report

2015

Annual FISMA Report

Chemical Safety Board

Section 1: Continuous Monitoring Management

1.1 Utilizing the ISCM maturity model definitions, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.

1.1.1 Please provide the D/A ISCM maturity level for the People domain.

Consistently Implemented (Level 3)

Comments: We based our assessment on CSB's self-assessment responses for the Continuous Monitoring maturity model collected by the audit team. Due to time constraints, auditors did not test the implementation or the effectiveness of the established guidance, or the operational effectiveness of the CSB information security program.

1.1.2 Please provide the D/A ISCM maturity level for the Processes domain.

Consistently Implemented (Level 3)

Comments: We based our assessment on CSB's self-assessment responses for the Continuous Monitoring maturity model collected by the audit team. Due to time constraints, auditors did not test the implementation or the effectiveness of the established guidance, or the operational effectiveness of the CSB information security program.

1.1.3 Please provide the D/A ISCM maturity level for the Technology domain

Consistently Implemented (Level 3)

Comments: We based our assessment on CSB's self-assessment responses for the Continuous Monitoring maturity model collected by the audit team. Due to time constraints, auditors did not test the implementation or the effectiveness of the established guidance, or the operational effectiveness of the CSB information security program.

1.1.4 Please provide the D/A ISCM maturity level for the ISCM Program Overall.

Consistently Implemented (Level 3)

Comments: We based our assessment on CSB's self-assessment responses for the Continuous Monitoring maturity model collected by the audit team. Due to time constraints, auditors did not test the implementation or the effectiveness of the established guidance, or the operational effectiveness of the CSB information security program.

1.2 Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model above.

N/A

Section 2: Configuration Management

Section 2: Configuration Management

2.1 Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

Comments: We based our assessment on the audit team collecting evidence of the existence of CSB's policies and procedures, CSB's self-assessment responses to the FY2015 FISMA metrics, and a Control Self-Assessment walkthrough, with CSB management, of selected information system security controls designated by DHS FISMA reporting metrics. Due to time constraints, auditors did not test the implementation or the effectiveness of the established guidance, or the operational effectiveness of the CSB information security program.

2.1.1 Documented policies and procedures for configuration management.

Yes

2.1.2 Defined standard baseline configurations.

Yes

2.1.3 Assessments of compliance with baseline configurations.

Yes

2.1.4 Process for timely (as specified in organization policy or standards) remediation of scan result findings.

Yes

2.1.5 For Windows-based components, USGCB secure configuration settings are fully implemented (when available), and any deviations from USGCB baseline settings are fully documented.

Yes

2.1.6 Documented proposed or actual changes to hardware and software baseline configurations.

Yes

2.1.7 Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI- 2).

Yes

Section 2: Configuration Management

2.1.8 **Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards. (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2).**

Yes

2.1.9 **Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches (NIST SP 800-53: CM-3, SI-2).**

Yes

2.2 **Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above.**

N/A

2.3 **Does the organization have an enterprise deviation handling process and is it integrated with an automated scanning capability?**

Yes

2.3.1 **Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented.**

Yes

Section 3: Identity and Access Management

3.1 **Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?**

Yes

Comments:

We based our assessment on the audit team collecting evidence of the existence of CSB's policies and procedures, CSB's self-assessment responses to the FY2015 FISMA metrics, and a Control Self-Assessment walkthrough, with CSB management, of selected information system security controls designated by DHS FISMA reporting metrics. Due to time constraints, auditors did not test the implementation or the effectiveness of the established guidance, or the operational effectiveness of the CSB information security program.

3.1.1 **Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1).**

Yes

Section 3: Identity and Access Management

3.1.2 Identifies all users, including Federal employees, contractors, and others who access organization systems (HSPD 12, NIST SP 800-53, AC-2).

Yes

3.1.3 Organization has planned for implementation of PIV for logical 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).

No

Comments: Although CSB does not have a formal plan for implementing PIV for logical access, CSB indicated it has planned for but not implemented logical access with PIV credentials. CSB stated its laptops and desktops all have PIV readers or the capability to use USB PIV readers. However, CSB stated it is still evaluating the risks of using PIV credentials for logical access, especially for investigators and other users in the field.

3.1.4 Organization has planned for implementation of 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).

Yes

3.1.5 Ensures that the users are granted access based on needs and separation-of-duties principles.

Yes

3.1.6 Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. IP phones, faxes, printers).

Yes

3.1.7 Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy.

Yes

3.1.8 Identifies and controls use of shared accounts.

Yes

3.2 Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was not noted in the questions above.

N/A

Section 4: Incident Response and Reporting

Section 4: Incident Response and Reporting

4.1 Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

Comments: We based our assessment on the audit team collecting evidence of the existence of CSB's policies and procedures, CSB's self-assessment responses to the FY2015 FISMA metrics, and a Control Self-Assessment walkthrough, with CSB management, of selected information system security controls designated by DHS FISMA reporting metrics. Due to time constraints, auditors did not test the implementation or the effectiveness of the established guidance, or the operational effectiveness of the CSB information security program.

4.1.1 Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1).

Yes

4.1.2 Comprehensive analysis, validation, and documentation of incidents.

Yes

4.1.3 When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).

Yes

4.1.4 When applicable, reports to law enforcement and the agency Inspector General within established timeframes.

Yes

4.1.5 Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).

Yes

4.1.6 Is capable of correlating incidents.

Yes

4.1.7 Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).

Yes

Section 4: Incident Response and Reporting

4.2 **Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.**

N/A

Section 5: Risk Management

5.1 **Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

Comments: We based our assessment on the audit team collecting evidence of the existence of CSB's policies and procedures, CSB's self-assessment responses to the FY2015 FISMA metrics, and a Control Self-Assessment walkthrough, with CSB management, of selected information system security controls designated by DHS FISMA reporting metrics. Due to time constraints, auditors did not test the implementation or the effectiveness of the established guidance, or the operational effectiveness of the CSB information security program.

5.1.1 **Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1.**

Yes

5.1.2 **Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800- 37, Rev. 1.**

Yes

5.1.3 **Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev.1.**

Yes

5.1.4 **Has an up-to-date system inventory.**

Yes

Comments: This attribute is being reported based on agency-managed systems only. We evaluated systems operated on behalf of CSB separately.

Section 5: Risk Management

5.1.5 **Categorizes information systems in accordance with government policies.**

Yes

5.1.6 **Selects an appropriately tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.**

Yes

5.1.7 **Implements the approved set of tailored baseline security controls specified in metric 5.1.6.**

Yes

5.1.8 **Assesses the security 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.**

Yes

5.1.9 **Authorizes information system operation 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.**

Yes

5.1.10 **Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.**

Yes

5.1.11 **Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).**

Yes

5.1.12 **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.**

Yes

5.1.13 **Security authorization package contains system security plan, security assessment report, POA&M, accreditation boundaries in accordance with government policies for organization information systems (NIST SP 800-18, 800-37).**

Yes

Section 5: Risk Management

5.1.14 The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.

N/A

5.1.15 For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems.

N/A

5.2 Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above.

N/A

Section 6: Security Training

6.1 Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

Comments: We based our assessment on the audit team collecting evidence of the existence of CSB's policies and procedures, CSB's self-assessment responses to the FY2015 FISMA metrics, and a Control Self-Assessment walkthrough, with CSB management, of selected information system security controls designated by DHS FISMA reporting metrics. Due to time constraints, auditors did not test the implementation or the effectiveness of the established guidance, or the operational effectiveness of the CSB information security program.

6.1.1 Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1).

Yes

6.1.2 Documented policies and procedures for specialized training for users with significant information security responsibilities.

No

Comments: CSB indicated that Individual Development Plans are reviewed annually for these users and include specific training requirements in specialized job-related functions. CSB stated it has also developed a draft order related to Individual Development Planning for not only IT personnel but for all our employees to ensure they acquire the necessary specialized training. CSB stated it will evaluate additional language in an update to its order on information security (Board Order 34) to include language that stipulates specialized training for users with significant information security responsibilities.

Section 6: Security Training

6.1.3 **Security training content based on the organization and roles, as specified in organization policy or standards.**

Yes

6.1.4 **Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training.**

Yes

6.1.5 **Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.**

Yes

6.1.6 **Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53).**

Yes

6.2 **Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.**

N/A

Section 7: Plan Of Action & Milestones (POA&M)

7.1 **Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

Comments:

We based our assessment on the audit team collecting evidence of the existence of CSB's policies and procedures, CSB's self-assessment responses to the FY2015 FISMA metrics, and a Control Self-Assessment walkthrough, with CSB management, of selected information system security controls designated by DHS FISMA reporting metrics. Due to time constraints, auditors did not test the implementation or the effectiveness of the established guidance, or the operational effectiveness of the CSB information security program.

7.1.1 **Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.**

Yes

Section 7: Plan Of Action & Milestones (POA&M)

7.1.2 **Tracks, prioritizes, and remediates weaknesses.**

Yes

7.1.3 **Ensures remediation plans are effective for correcting weaknesses.**

Yes

7.1.4 **Establishes and adheres to milestone remediation dates and provides adequate justification for missed remediation dates.**

Yes

7.1.5 **Ensures resources and ownership are provided for correcting weaknesses.**

Yes

7.1.6 **POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk- based decision to not implement a security control) (OMB M-04-25).**

Yes

7.1.7 **Costs associated with remediating weaknesses are identified in terms of dollars (NIST SP 800-53: PM-3; OMB M-04-25).**

Yes

7.1.8 **Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53:CA-5; OMB M-04-25).**

Yes

7.2 **Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above.**

N/A

Section 8: Remote Access Management

Section 8: Remote Access Management

8.1 **Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

Comments: We based our assessment on the audit team collecting evidence of the existence of CSB's policies and procedures, CSB's self-assessment responses to the FY2015 FISMA metrics, and a Control Self-Assessment walkthrough, with CSB management, of selected information system security controls designated by DHS FISMA reporting metrics. Due to time constraints, auditors did not test the implementation or the effectiveness of the established guidance, or the operational effectiveness of the CSB information security program.

8.1.1 **Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17).**

Yes

8.1.2 **Protects against unauthorized connections or subversion of authorized connections.**

Yes

8.1.3 **Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1).**

Yes

8.1.4 **Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1).**

Yes

8.1.5 **Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.**

Yes

8.1.6 **Defines and implements encryption requirements for information transmitted across public networks.**

Yes

8.1.7 **Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.**

Yes

Section 8: Remote Access Management

8.1.8 **Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines).**

Yes

8.1.9 **Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4).**

Yes

8.1.10 **Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1; NIST SP 800-53, PS-6).**

Yes

8.2 **Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.**

N/A

8.3 **Does the organization have a policy to detect and remove unauthorized (rogue) connections?**

Yes

Section 9: Contingency Planning

9.1 **Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

Comments:

We based our assessment on the audit team collecting evidence of the existence of CSB's policies and procedures, CSB's self-assessment responses to the FY2015 FISMA metrics, and a Control Self-Assessment walkthrough, with CSB management, of selected information system security controls designated by DHS FISMA reporting metrics. Due to time constraints, auditors did not test the implementation or the effectiveness of the established guidance, or the operational effectiveness of the CSB information security program.

9.1.1 **Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1).**

Yes

Section 9: Contingency Planning

9.1.2 **The organization has incorporated the results of its system's Business Impact Analysis and Business Process Analysis into the appropriate analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan (NIST SP 800-34).**

Yes

9.1.3 **Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34).**

Yes

9.1.4 **Testing of system-specific contingency plans.**

Yes

9.1.5 **The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).**

Yes

9.1.6 **Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

9.1.7 **Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans.**

Yes

9.1.8 **After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).**

Yes

9.1.9 **Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for systems that require them (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

9.1.10 **Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

9.1.11 **Contingency planning that considers supply chain threats.**

Yes

Section 9: Contingency Planning

9.2 **Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.**

N/A

Section 10: Contractor Systems

10.1 **Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including for organization systems and services residing in a cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

Comments: We based our assessment on the audit team collecting evidence of the existence of CSB's policies and procedures, CSB's self-assessment responses to the FY2015 FISMA metrics, and a Control Self-Assessment walkthrough, with CSB management, of selected information system security controls designated by DHS FISMA reporting metrics. Due to time constraints, auditors did not test the implementation or the effectiveness of the established guidance, or the operational effectiveness of the CSB information security program.

10.1.1 **Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities (including other government agencies), including organization systems and services residing in a public, hybrid, or private cloud.**

Yes

10.1.2 **The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and compliant with FISMA requirements, OMB policy, and applicable NIST guidelines (NIST SP 800-53: CA-2).**

No

Comments: CSB indicated it receives financial and human resources services from other agencies in the federal government and had not included these in the System Security Plan. CSB stated it will work to add these to the updated System Security Plan and acquire the necessary supporting documentation regarding the servicing agency's implementation of security controls.

Section 10: Contractor Systems

10.1.3 A complete inventory of systems operated on the organization's behalf by contractors or other entities, (including other government agencies), including organization systems and services residing in public, hybrid, or private cloud.

No

Comments: CSB indicated it receives financial and human resources services from other agencies in the federal government and had not included these in the System Security Plan. CSB stated it will work to add these to the updated System Security Plan and acquire the necessary supporting documentation regarding the servicing agency's implementation of security controls.

10.1.4 The inventory identifies interfaces between these systems and organization- operated systems (NIST SP 800-53: PM-5).

Yes

10.1.5 The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.

Yes

10.1.6 The inventory of contractor systems is updated at least annually.

No

10.2 Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.

N/A

CSB Response to Discussion Draft Report

January 11, 2015

Rudy Brevard
Director, IRM Audits
U.S. Environmental Protection Agency
Office of Inspector General
1200 Pennsylvania Ave
Washington, DC 20460

Dear Mr. Brevard:

Thank you for the opportunity to review and comment on the January 7, 2015, discussion draft of the CSB's compliance with the Federal Information Security Modernization Act (FISMA) for fiscal year 2015.

The CSB takes information security seriously and works diligently each year to address the recommendations from the FISMA audits. The CSB agrees overall with the findings and recommendations from this most recent report; however, the following are some comments on the three main findings on the CSB's planned actions in response to these recommendations.

Identity and Access Management

CSB has not planned for implementation of PIV cards for logical access.

The CSB has planned for but not implemented logical access with PIV credentials. CSB laptops and desktops all have PIV readers or the capability to use USB PIV readers. However, the agency is still evaluating the risks of using PIV credentials for logical access, especially for investigators and other users in the field.

Security Training

CSB does not have policies or procedures that specifies the specialized training requirements for users with significant information security responsibilities.

Individual Development Plans are reviewed annually for these users and include specific training requirements in specialized job-related functions. The CSB has also developed a draft order related to Individual Development Planning for not only IT personnel but for all our employees to ensure they acquire the necessary specialized training. We will evaluate additional language in an update to our order on information security (Board Order 34) to include language that stipulates specialized training for users with significant information security responsibilities.

U.S. Chemical Safety and Hazard Investigation Board

Contractor Systems

CSB lacks an inventory of systems that are operated on behalf of the agency and does not have assurance that the security controls for systems operated on behalf of the agency are effectively implemented.

The CSB receives financial and HR services from other agencies in the federal government and had not included these in the System Security Plan (SSP). We will work to add these to the updated SSP and acquire the necessary supporting documentation regarding the servicing agency's implementation of security controls.

If you or your staff have any questions about this response, please feel free to contact our CIO, Charlie Bryant, at 202-261-7666.

Sincerely,

/s/
Vanessa Allen Sutherland
Chairperson and Board Member

Appendix C

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
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