U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

U.S. Chemical Safety Board

Cybersecurity Act of 2015 Report: CSB's Policies and Procedures to Protect Systems With Personally Identifiable Information

Report No. 16-P-0254 **August 1, 2016**

REDACTED VERSION FOR PUBLIC RELEASE

The full version of this report contained controlled unclassified information. This is a redacted version of that report, which means the controlled unclassified information has been removed. The redactions are clearly identified in the report.

Report Contributors:

Rudolph M. Brevard
Charles M. Dade
Nancy Dao
Iantha Maness
Christina N. Nelson

Abbreviations

ACL	Access Control List
CIO	Chief Information Officer
CSB	U.S. Chemical Safety and Hazard Investigation Board
OIG	Office of Inspector General
PII	Personally Identifiable Information

Cover photo: OIG image of an RSA SecurID token atop a laptop.

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

16-P-0254
August 1, 2016

At a Glance

Why We Did This Review

We performed this audit to assess to what extent the U.S. Chemical Safety and Hazard Investigation Board (CSB) implemented information system security policies and procedures to protect CSB systems that provide access to national security or Personally Identifiable Information (PII) as outlined in Section 406 of the Cybersecurity Act of 2015.

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.

Cybersecurity Act of 2015 Report: CSB's Policies and Procedures to Protect Systems With Personally Identifiable Information

What We Found

Section 406 of the Cybersecurity Act of 2015 calls for Inspectors General of agencies with covered systems to report on several aspects of the covered systems' information system security controls. The term "covered system" means a national security system as defined in 40 U.S.C. § 11103 or a federal computer system that provides access to PII.

CSB has one system that contains sensitive PII. Safeguarding such information in the possession of the government and preventing its breach is essential to ensuring CSB retains the trust of the American public.

CSB identified one covered system that contains sensitive PII covered by provisions of the act. CSB does not have any national security information systems.

The act requires Inspectors General to report on the areas identified in the bullets below. We provided information in the following eight areas based on the requirements outlined in the act for CSB's covered system:

- Description of logical access policies and practices.
- Description of the logical access controls and multi-factor authentication used to govern privileged users access.
- Reasons for not using logical access controls and multi-factor authentication if applicable.
- Policies and procedures used to conduct inventories of software and licenses.
- Capabilities utilized to monitor and detect exfiltration and other threats.
- Description of how monitoring and detecting capabilities are utilized.
- Reasons why monitoring and detecting capabilities are not used if applicable.
- Description of policies and procedures used to ensure entities and contractors providing services to CSB are implementing the information security management practices identified in the act.

We worked closely with CSB throughout this audit to obtain the data in this report. We issued a draft report containing our conclusions, and subsequently briefed CSB representatives on the audit results. CSB agreed with our results, and did not provide a written response to this report.

The full version of this report contained controlled unclassified information. This is a redacted version of that report, which means the controlled unclassified information has been removed. The redactions are clearly identified in the report.

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

THE INSPECTOR GENERAL

August 1, 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 a report on our audit pertaining to the Cybersecurity Act of 2015, as outlined by Section 406 of the act. We believe the evidence obtained provides a reasonable basis for our findings and conclusions and, in all material respects, meets the reporting requirements prescribed by Section 406 of the act.

The full version of this report contained controlled unclassified information. This is a redacted version of that report, which means the controlled unclassified information has been removed. The redactions are clearly identified in the report.

You are not required to provide a written response to this final report. In accordance with Section 406 of the Cybersecurity Act of 2015, we are forwarding the full version of this report to the appropriate committees of Congress.

Sincerely,

Arthur A. Elkins Jr.

Table of Contents

Appendix

Purpose

The Office of Inspector General (OIG) performed this audit to determine to what extent the U.S. Chemical Safety and Hazard Investigation Board (CSB) implemented information system security policies and procedures to protect CSB's systems that provide access to national security or Personally Identifiable Information (PII), as outlined by Section 406 of the Cybersecurity Act of 2015.[1]

Background

Section 406 of the Cybersecurity Act requires Inspectors General to submit to the appropriate congressional committees a report providing specific information collected from the agency regarding the protection of covered systems.

A covered system is a national security system as defined in 40 U.S.C. § 11103 or a federal computer system that provides access to PII.

CSB is an independent federal agency charged with investigating industrial chemical accidents. CSB is headquartered in Washington, D.C.; its Western Region Office is located in a federal center complex in Denver, Colorado. As of February 2016, CSB had identified only one system that contained sensitive PII.

Responsible Offices

CSB's Chairperson is responsible for agency administration. CSB's Office of Administration is responsible for the information technology security program. The Chief Information Officer (CIO) and Deputy CIO are responsible for making risk management decisions regarding deficiencies; their potential impact on controls; and the confidentiality, integrity and availability of systems.

Scope and Methodology

We conducted this audit from March through July 2016 at CSB's headquarters in Washington, D.C., 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 upon the audit objective. We believe that the information obtained provides a reasonable basis for our conclusions based on our audit objective.

We collected CSB's policies and procedures related to the areas being reported under this statute. To gain an understanding of the service provider's implementation of its information security program, we reviewed the independent auditor's report that documents the review of the service provider's processes for protecting the data received by CSB. We also reviewed the Memorandum of

[1] Cybersecurity Act of 2015, Section 406, *Federal Computer Security*; Pub. L. No. 2015-114-113; 129 Stat. 2574.

Understanding between CSB and the service provider to understand the roles and responsibilities for protecting the covered system and network connection. We reviewed CSB's only information system security plan to identify systems that contained national security information or PII. Because the security plan did not include what type of information was included in the systems, we obtained the information directly from the CIO.

The CIO indicated CSB had only one system that contained PII, and did not have any systems with national security information. We interviewed CSB's CIO regarding the only system with sensitive PII. Where CSB did not document its policies, procedures and practices, we relied upon information provided by CSB's CIO to explain the respective processes necessary to complete the report on the covered system required by Section 406 of the Cybersecurity Act. Where the act asked if appropriate standards were followed, our audit work consisted of determining whether CSB developed its policies and procedures using current federal guidance.

Prior Audits

We took into account three applicable prior reports, which are summarized below.

1. **Fiscal Year 2015 Federal Information Security Modernization Act Report: Status of CSB's Information Security Program (Report No. 16-P-0086, dated January 27, 2016)**: CSB fully met seven of the 10 information security program areas specified by the fiscal year 2015 Department of Homeland Security Federal Information Security Modernization Act reporting metrics: (1) Continuous Monitoring Management, (2) Configuration Management, (3) Incident Response and Reporting, (4) Risk Management, (5) Plan of Action and Milestones, (6) Remote Access Management, and (7) Contingency Planning. For the remaining three areas, we indicated management attention was needed to improve processes that potentially could place these areas at risk:

    - **Identity and Access Management.** CSB had not implemented the use of personal identification verification cards for logical access into its systems.

    - **Security Training.** CSB did not have policies or procedures that specified the specialized training requirements for users with significant information security responsibilities.

    - **Contractor Systems.** CSB lacked an inventory of systems operated on behalf of the agency, and did not have assurance that security controls for those systems were effectively implemented.

2. **CSB Needs Better Security Controls to Protect Critical Data Stored on Its Regional Servers (Report No. 16-P-0035, dated November 5, 2015)**: We reported that CSB should strengthen physical and environmental protection controls for its Western Regional Office server room. CSB also should take steps to implement the remaining four recommendations from the prior year report to resolve security deficiencies cited. CSB also had not taken steps to establish access control rosters and physical access logs to control and monitor access to the Western Regional Office server room. We made seven recommendations. During the course of our audit, CSB took immediate steps to address one of the recommendations. We plan to follow up to determine the status of the remaining six recommendations as a part of the fiscal year 2016 Federal Information Security Modernization Act audit.

3. **Key Aspects of CSB Information Security Program Need Improvement (Report No. 15-P-0073, 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, its vulnerability testing process, and internal controls over its information technology inventory. We recommended that CSB update and maintain its system security plan, implement a risk management framework, create a visitor access record for the server room, formally accept risk of unimplemented privacy and security controls as well as vulnerabilities, and develop a process for orderly shutdown of critical information technology assets. We also recommended that CSB create plans to remediate systems with known vulnerabilities, improve its inventory control practices to ensure personnel do not perform incompatible duties, provide policies and procedures for safeguarding inventory, review and document lost items, and recover costs for lost items due to employee negligence. In total, we made 17 recommendations, and CSB management agreed with all recommendations. Our follow-up audit determined that CSB took sufficient actions to address 13 of the recommendations. We plan to follow up to determine the status of the remaining four recommendations as a part of the fiscal year 2016 Federal Information Security Modernization Act audit.

Results of Review

In response to the information requested under Section 406 of the Cybersecurity Act, we determined that CSB:

- Has logical access policies and procedures for the covered system. However, the authorities listed in one of the documents were outdated, and the document is in the process of being updated.
- Uses logical access controls for privileged users to access its covered system. [redacted]

"**Multi-factor authentication** – The use of not fewer than two authentication factors, such as:

(a) Something that is known to the user, such as a password or personal identification number.
(b) An access device that is provided to the user, such as a cryptographic identification device or token.
(c) A unique biometric characteristic of the user."

"**Privileged User** – A user who has access to system control, monitoring or administrative functions."

Cybersecurity Act of 2015, Section 406(a)(4-5)

We limited our review to the reporting requirements under the Cybersecurity Act of 2015. We are providing the following information based on the requirements outlined in Section 406(b)(2) of the act.

(A) A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.

Logical access control is a process of granting or denying specific requests to obtain and use information and related information-processing services. CSB has two documents that cover logical access controls, as described in Table 1.

Table 1: CSB policies and procedures related to logical access, and descriptions

CSB policy title and date	Description
Board Order 034, Information Technology Security Program, October 2008	This order establishes an agencywide information technology security program for CSB and sets forth the board's policy on information technology security.
U.S. Chemical Safety and Hazard Investigation Board Information System Security Plan, January 2016	The Information System Security Plan documents the current and planned controls for the system and addresses security concerns that may affect the system's operating environment.

Source: OIG analysis.

There are several authorities identified in CSB's Board Order 34. Our review of five of these authorities determined that the authorities listed are outdated. Of the five authorities reviewed, only two of the authorities referenced current federal guidance. The CIO indicated that Board Order 34 is in the process of being updated.

[redacted]

According to the CSB CIO, [redacted]

- [redacted]
- [redacted]
- [redacted]

In addition, Board Order 34 lists the following access control procedure:

[redacted]

Additionally, per the CIO:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

(C) If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.

[redacted]

(D)(i) [A description of] the policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

[redacted] However, CSB Board Order 34 states:

> Users must install and operate only software that is properly licensed for use at the CSB and that has been approved for CSB use by the IT Manager.

[redacted]

[redacted]

(D)(ii) [A description of the] capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including: data loss prevention capabilities; forensics and visibility capabilities; or digital rights management capabilities.

We could not find evidence of data loss prevention, forensics and visibility, or digital rights management capability procedures within CSB's Board Order 34 or Information System Security Plan. However, upon inquiry, CSB described the following capabilities to monitor and detect exfiltration and other threats (Table 2).

Table 2: CSB capabilities to monitor and detect exfiltration and other threats

Data loss prevention capabilities	Forensics and visibility capabilities	Digital rights management capabilities
[redacted]	[redacted]	[redacted]

Source: OIG analysis.

(D)(iii) A description of how the covered agency is using the capabilities described in clause (ii).

[redacted]

(D)(iv) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.

CSB uses capabilities to detect threats and, therefore, this request is not applicable.

(E) A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph (D).

[redacted]

We reviewed the independent service auditor's report provided by KPMG, LLC, *Report on the U.S. Department of Interior's Description of Its Federal Personnel and Payroll System and the Suitability of the Design and Operating Effectiveness of Its Controls* (SSAE 16 – Type 2 Report), issued for the period July 1, 2014, to June 30, 2015. The independent auditor's opinion stated:

> In our opinion, in all material respects, based on the criteria described in Interior's assertions, (1) the description fairly presents the system was designed and implemented throughout the period July 1, 2014 through June 30, 2015, (2) the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved …, and (3) the controls tested … if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period July 1, 2014 through June 30, 2015.

CSB Response to the Draft Report and OIG Evaluation

Due to the critical milestones necessary to meet the act's mandatory reporting date, we worked closely with CSB representatives throughout this audit to obtain the data contained within this final report, and to ensure CSB was familiar with our findings and the issues addressed. We had provided CSB with a draft report containing our conclusions. On July 20, 2016, we met with CSB to discuss the factual accuracy of our draft report. CSB verbally concurred with the information presented in our draft report and indicated it will not provide a written response.

Appendix A

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
General Counsel, U.S. Chemical Safety and Hazard Investigation Board