



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

OFFICE OF
INSPECTOR GENERAL

March 14, 2016

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

Dear Ms. Sutherland:

The Office of Inspector General (OIG) for the U.S. Environmental Protection Agency plans to begin fieldwork for an audit of the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) compliance with the mandated "Inspector General Report on Covered Systems," as outlined in the Cybersecurity Act of 2015.

The OIG's audit objective is to determine to what extent the CSB implemented information system security policies and procedures to protect CSB systems that provide access to national security or personally identifiable information, as outlined by Title IV, Section 406 of the Cybersecurity Act of 2015. The OIG plans to conduct its work at CSB headquarters. Applicable generally accepted government auditing standards will be used in conducting our project. The anticipated benefit of this project is to help CSB improve business practices and accountability.

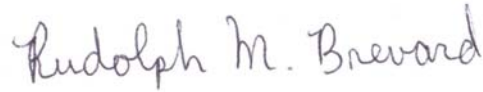
We will contact you to arrange a mutually agreeable time to discuss the audit scope and objective. We would also be particularly interested in any areas of concern that you may have. We will answer any questions you may have about the project process, reporting procedures, methods used to gather and analyze data, and what we should expect of each other during the course of the project. During the audit, we will provide updates on a regular basis by email and/or during meetings with CSB staff.

As we indicated in our February 25, 2016, email to the CSB's Chief Information Officer, we have enclosed a list outlining the specific information that we need from the CSB in order to complete the Inspector General Report on Covered Systems. To ensure the success and timely completion of this project, the CSB should provide the OIG with the information requested in the enclosure within 2 weeks from the date of this letter.

We respectfully note that the OIG is authorized by the Inspector General Act of 1978 to have timely access to personnel and all materials necessary to complete its objectives. We will request your resolution if an agency employee or contractor refuses to provide requested records to the OIG, or otherwise fails to cooperate with the OIG. We may report unresolved access matters to appropriate CSB officials and include the incident in the Semiannual Report to Congress.

If you or your staff have any questions, please contact me at (202) 566-0893 or brevard.rudy@epa.gov; or Chuck Dade, Project Manager, at (202) 566-2575 or dade.chuck@epa.gov.

Sincerely,



Rudolph M. Brevard, Director
Information Resources Management Audits

Enclosures

1. Request for Information
2. Excerpt of the Definitions From the Cybersecurity Act of 2015

cc: Kristen Kulinowski, Ph.D., Board Member, CSB
Manuel Ehrlich, Board Member, CSB
Rick Engler, Board Member, CSB
Anna Brown, Director of Administration and Audit Liaison, CSB
Allen Smith, Deputy Director of Administration, CSB
Hillary Cohen, Communications Manager, CSB
Charlie Bryant, Chief Information Officer, CSB
Ron LaRoche, Deputy Chief Information Officer, CSB
Arthur A. Elkins Jr., Inspector General
Charles Sheehan, Deputy Inspector General
Aracely Nunez-Mattocks, Chief of Staff, Office of Inspector General
Alan Larsen, Counsel to the Inspector General
Kevin Christensen, Assistant Inspector General for Audit
Carolyn Copper, Assistant Inspector General for Program Evaluation
Patrick Sullivan, Assistant Inspector General for Investigations
Richard Eyermann, Deputy Assistant Inspector General for Audit
Jennifer Kaplan, Deputy Assistant Inspector General for Congressional and Public Affairs
Jeffrey Lagda, Congressional and Media Liaison, Office of Inspector General

Request for Information

Information Requested for the Audit of the CSB's Protection of Systems With Access to National Security or Personally Identifiable Information

1. Please provide within 2 weeks from the date of the letter, an electronic copy of your response to the following requested information (noted in bold type).
2. Please provide in electronic format, within 2 weeks from the date of the letter, copies of CSB policies and procedures noted below.

Extract From Cybersecurity Act of 2015

(b) INSPECTOR GENERAL REPORTS ON COVERED SYSTEMS.—

- (1) IN GENERAL.—Not later than 240 days after the date of enactment of this Act, the Inspector General of each covered agency shall submit to the appropriate committees of jurisdiction in the Senate and the House of Representatives a report, which shall include information collected from the covered agency for the contents described in paragraph (2) regarding the Federal computer systems of the covered agency.
- (2) CONTENTS.—The report submitted by each Inspector General of a covered agency under paragraph (1) shall include, with respect to the covered agency, the following:
 - (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.

Please provide:

- (1) **A description of the logical access policies and practices CSB uses to access the WebTA timekeeping system.**
- (2) **Electronic copies of CSB policies and procedures associated with the logical access practices.**

- (B) A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.

Please provide:

- (1) **A description and a list of the logical access controls that CSB uses for privileged users to access the WebTA timekeeping system.**
- (2) **A description of the Multi-factor authentication that CSB uses for privileged users to access the WebTA timekeeping system.**

- (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.

- (1) If the CSB is not using logical access controls to access the WebTA timekeeping system, please provide a description of the reasons for not using logical access controls.**
- (2) If the CSB is not using multi-factor authentication to access the WebTA timekeeping system, please provide a description of the reasons for not using multi-factor authentication.**

(D) A description of the following information security management practices used by the covered agency regarding covered systems:

- (i) 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.

Please provide:

- (1) A description of the policies and practices that CSB follows to conduct inventories of the software present on the covered systems and the licenses associated with such software.**
- (2) Electronic copies of CSB policies and procedures associated with the practices followed for conducting inventories of the software present, and the licenses associated with such software practices.**

- (ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including—
 - (I) data loss prevention capabilities;
 - (II) forensics and visibility capabilities; or
 - (III) digital rights management capabilities.

Please provide a description of the capabilities CSB utilizes to monitor and detect exfiltration and other threats, including: (1) data loss prevention capabilities; (2) forensics and visibility capabilities; and (3) digital rights management capabilities.

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

Please provide a description of how the CSB is using the capabilities described in clause (ii).

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

If the CSB is not utilizing capabilities described in clause (ii), please provide a description of the reasons for not utilizing such capabilities.

(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).

Please provide:

- (1) A description of the policies and practices CSB uses 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).**
- (2) Electronic copies of CSB policies and procedures associated with these policies and practices.**

Excerpt From Cybersecurity Act of 2015

SEC. 406. FEDERAL COMPUTER SECURITY.

(a) DEFINITIONS.—In this section:

- (1) COVERED SYSTEM.—The term “covered system” shall mean a national security system as defined in section 11103 of title 40, United States Code, or a Federal computer system that provides access to personally identifiable information.
- (2) COVERED AGENCY.—The term “covered agency” means an agency that operates a covered system.
- (3) LOGICAL ACCESS CONTROL.—The term “logical access control” means a process of granting or denying specific requests to obtain and use information and related information processing services.
- (4) MULTI-FACTOR AUTHENTICATION.—The term “multifactor authentication” means the use of not fewer than 2 authentication factors, such as the following:
 - (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.
- (5) PRIVILEGED USER.—The term “privileged user” means a user who has access to system control, monitoring, or administrative functions.