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

OFFICE OF
INSPECTOR GENERAL

May 19, 2014

The Honorable Rafael Moure-Eraso, Ph.D
Chairperson and Chief Executive Officer
U.S. Chemical Safety and Hazard Investigation Board
2175 K Street, NW, Suite 400
Washington, D.C. 20037-1809

Dear Dr. Moure-Eraso:

The U.S. Environmental Protection Agency (EPA) Office of Inspector General (OIG) plans to begin fieldwork for an audit of the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) compliance with the Federal Information Security Management Act (FISMA). This project is included in our fiscal year 2014 audit plan to contribute to improving CSB's business practices and accountability.

The purpose of this memorandum is to confirm our mutual understandings on the objectives and scope of the audit of CSB's compliance with FISMA, as well as responsibilities of the CSB and the EPA OIG during the project. The EPA OIG plans to conduct its work at CSB headquarters and Denver offices. The project will be conducted using applicable *Generally Accepted Government Auditing Standards*. The anticipated benefit of this project is to help CSB improve CSB's business practices and accountability.

The EPA OIG's objective is to evaluate the implementation and effectiveness of CSB information security practices as it relates to complying with FISMA.

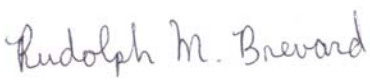
During the audit, we will continue to provide updates on this project on a regular basis by email and/or during meetings with CSB staff.

To ensure the success and timely completion of this project, the CSB should provide the EPA OIG with the information listed in the enclosure by June 6, 2014.

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.

If you or your staff have any questions, please contact me at (202) 566-0893 or brevard.rudy@epa.gov; or Michael Goode, Project Manager, at (215) 814-2314 or goode.michael@epa.gov.

Sincerely,



Rudolph M. Brevard
Director, Information Resources Management Audits

Enclosure

cc: Mark Griffon, Board Member, CSB
Beth Rosenberg, Board Member, CSB
Daniel M. Horowitz, Managing Director, CSB
Richard Loeb, Office of General Counsel, CSB
Christopher Warner, Senior Counsel to the Chair, CSB
John Lau, Deputy Managing Director, CSB
Anna Brown, Director, Office of Administration, CSB
Hillary Cohen, Office of Congressional, Public, and Board Affairs, CSB
Arthur A. Elkins Jr., Inspector General
Charles Sheehan, Deputy Inspector General
Aracely Nunez-Mattocks, Chief of Staff, OIG
Alan Larsen, Counsel to the Inspector General
Kevin Christensen, Acting Assistant Inspector General for Audit
Patricia Hill, Assistant Inspector General for Mission Systems
Carolyn Copper, Assistant Inspector General for Program Evaluation
Patrick Sullivan, Assistant Inspector General for Investigations
Jennifer Kaplan, Deputy Assistant Inspector General for Congressional and Public Affairs

Enclosure

Information Requested for the FY14 CSB FISMA Audit

Please provide the following information by electronic format by May 29, 2014, or hardcopies brought to the Entrance Conference for the FY14 CSB FISMA Audit:

1. Points of contact for CSB personnel response for information security at all CSB locations.
2. CSB policies and procedures related to inventory of information technology assets and systems, and policies and procedures related to management oversight of CSB server rooms.
3. CSB network architecture diagram (diagram should depict all public facing servers, intranet servers, connections to external business partners on public or private circuits, and connections to all CSB physical locations)
4. CSB system inventory (listing should include applications or services that are contractor owned or operated on behalf of CSB and the listing of all applications grouped under the consolidated security plans).
5. Inventory of information technology assets (e.g., routers, servers, desktops, laptops, blackberries, RSA tokens, etc.). Inventory should include current location of the information technology asset.