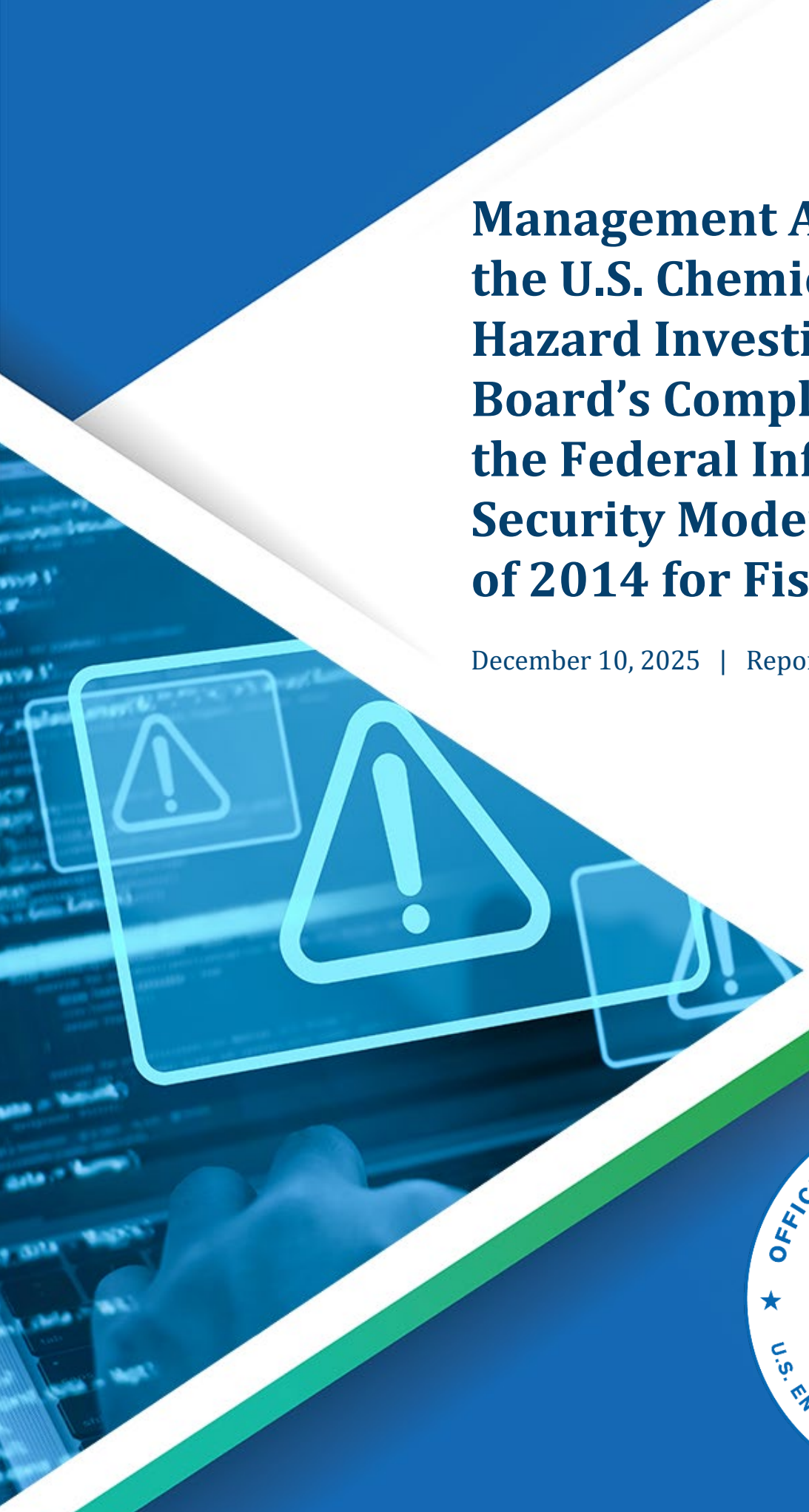
Management Alert: Audit of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2025

December 10, 2025 | Report No. 26-N-0004



Abbreviations

CSB	U.S. Chemical Safety and Hazard Investigation Board
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Modernization Act
OIG	Office of Inspector General

Cover Image

A technology-themed image with the multiple "alert" symbol, representing that the CSB's cybersecurity program has security concerns with user access, audit logs, and inventory records that may have a significant impact on the confidentiality, integrity, and availability of the Agency's IT resources. (EPA OIG image)

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

December 10, 2025

Mr. Steve Owens
Chairperson
U.S. Chemical Safety and Hazard Investigation Board
1750 Pennsylvania Avenue NW, Suite 910
Washington, D.C. 20006

Dear Mr. Owens:

The Office of Inspector General for the U.S. Environmental Protection Agency, which also provides oversight for the U.S. Chemical Safety and Hazard Investigation Board, or CSB, contracted with the independent accounting firm SB & Company LLC to initiate an audit of the CSB's compliance with the Federal Information Security Modernization Act of 2014, or FISMA.

While conducting the audit of the CSB's compliance with FISMA for fiscal year 2025, OIG Project No. OA-FY25-0042, SB & Company identified issues that may have a significant impact on the confidentiality, integrity, and availability of the CSB's information technology resources. The OIG decided to issue this management alert to inform the CSB of these security concerns because they could affect the CSB's ability to fulfill its mission and carry out its obligations under FISMA and Office of Management and Budget Memorandum M-25-04. See SB & Company's enclosed memorandum documenting the identified issues.

We agree with SB & Company's findings and adopt them as our own.

You are not required to respond to this report because this report contains no recommendations. If you submit a response, however, it will be posted on the OIG's website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the requirements of section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal along with corresponding justification.

We will post this report to our website at https://www.epa.gov/oig.

Sincerely,

Nicole N. Murley

Nicole N. Murley
Acting Inspector General

Enclosure

cc: Steven Messer, Senior Advisor and Acting General Counsel, CSB
Sylvia Johnson, Board Member, CSB
Sabrina Morris, EPA OIG Liaison and Director of Administration/Board Affairs, CSB

SB & COMPANY, LLC
KNOWLEDGE • QUALITY • CLIENT SERVICE

MEMO

To: US Chemical Safety and Hazard Investigation Board
Date: August 22, 2025
Updated: August 29, 2025
From: Julie Paris, SB & Company, LLC

During the review of the CSB's cyber security program for FISMA, the following issues were identified that may have significant impact on the confidentiality, integrity, and availability of the agency's IT resources. Improvements are needed related to managing privileged user access, availability of audit logs and maintaining an accurate inventory. We believe these security concerns should be brought to your attention before we issue our FISMA report. Our report may include matters not contained in this memo.

1. The CSB did not properly monitor and track privileged user access or retain sufficient audit logs of individuals with system privileges. Specifically, the CSB did not adequately manage access to global administrator accounts, which provides privileged users with the highest level of system access. Also, the CSB did not provide evidence that sufficient audit logs are maintained for monitoring and tracking user access and the historical usage of privileged accounts. The current system only retains audit logs for 30 days. If the CSB's privileged accounts are misused or compromised by threat actors, they will lack historical information to aid in their investigation.

   These security issues undermine the CSB's ability to verify whether their privileged roles are appropriately granted or disabled when no longer needed. Without retaining a historical record of global administrators with system access, it becomes difficult to demonstrate:
   - Enforcement of the minimum access permissions required to perform specific tasks.
   - Compliance with internal access control policies.
   - Completion of access reviews for high-risk roles.
   - Documentation of an audit trail of privileged user activity.

   Left uncorrected, this increases the risk of unauthorized access, misuse of privileged accounts, and audit findings related to access management control weaknesses. Documenting both the granting and removal of global administrator access is essential for maintaining a secure and compliant environment.

2. The CSB did not demonstrate that they maintained a comprehensive and accurate inventory of all IT assets connected to its network. Although the CSB has Asset Management software, it does not have a documented process for regularly reviewing and validating their inventory. Our review of the inventory management dashboard revealed that over 50% of the software on the devices is classified as unknown. The absence of a complete inventory hinders effective cybersecurity risk management, as it prevents full visibility into potential vulnerabilities, unauthorized devices, and configuration compliance. Without an accurate inventory, it is difficult to enforce security controls, detect unauthorized changes, or respond effectively to security incidents.

Whistleblower Protection

U.S. Environmental Protection Agency

The whistleblower protection coordinator's role is to educate Agency employees about prohibitions against retaliation for protected disclosures and the rights and remedies against retaliation. For more information, please visit our website.

Contact us:

Congressional & Media Inquiries: OIG.PublicAffairs@epa.gov

EPA OIG Hotline: OIG.Hotline@epa.gov

Web: epa.gov/oig

Follow us:

X: @epaoig

LinkedIn: linkedin.com/company/epa-oig

YouTube: youtube.com/epaoig

Instagram: @epa.ig.on.ig

www.epa.gov/oig