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

THE INSPECTOR GENERAL

September 22, 2022

Steve Owens
Board Member and Interim Executive Authority
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 evaluation of the CSB's compliance with the Federal Information Security Modernization Act of 2014, or FISMA.

While conducting the evaluation of the CSB's compliance with FISMA for fiscal year 2022, Project No. OA-FY22-0136, SB & Company identified issues that may have a significant impact on the confidentiality, integrity, and availability of the CSB's data. The OIG decided to issue this management alert to inform the CSB of these vulnerabilities because they could impact the CSB's ability to fulfill its mission and carry out its obligations under FISMA and Office of Management and Budget Memorandum M-22-05. See SB & Company's enclosed memorandum documenting the identified issues.

This memorandum contains SB & Company's findings. 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 accessibility 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 www.epa.gov/oig.

Sincerely,

Sean W. O'Donnell

Sean W. O'Donnell

Enclosure

cc: David LaCerte, Senior Advisor and Executive Counsel, CSB
Dr. Sylvia Johnson, Board Member, CSB
Stephen Klejst, Executive Director of Investigations and Recommendations, CSB
Michele Bouziane, Acting General Counsel, CSB
Sabrina Morris, Acting Director of Administration, CSB

SB & COMPANY, LLC
KNOWLEDGE • QUALITY • CLIENT SERVICE

MEMO

Subject: US Chemical Safety and Hazard Investigation Board Cyber Security Program
Date: July 7, 2022
Updated: August 4, 2022
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 that we believe should be brought to your attention before we issue our report for this review. Our report may include matters not contained in this memo.

- The servers are not being backed up to tape and transported off site. The last backup that was transported off site was in April 2022. We were informed that offsite backups have been discontinued due to the time that it takes to perform this function. In the event that the servers located at headquarters are damaged or destroyed, several months of data will be lost, impacting the agency's ability to fulfill its obligations. Subsequent to our testing, we received information from the CSB that indicated offsite backup was performed for most servers between July 14 and July 19, 2022 and sent to their offsite storage vendor on August 1, 2022. Additionally, the CSB is in the process of contracting with Veeam Government Solutions to implement the VEEAM Backup Application, which will provide an automated solution for both onsite and offsite backups. Until offsite tape backups are performed regularly or the VEEAM Backup Application is implemented, there is the potential exposure of not being able to recover data if the data on the system is lost.
- Vulnerability scanning of the network has been discontinued. The lack of periodic (monthly) scanning may prevent vulnerabilities from being identified and remediated in a timely manner. Unremediated vulnerabilities increase the risk of successful cyber attacks which may result in the loss of data and disruption to agency operations.
- A risk assessment has not been performed in the past 24 months. A risk assessment is essential in identifying threats to the agency and enabling the agency to mitigate the risks identified.
- Though not part of the FISMA review, it was brought to our attention that the operating systems running many of the agency's servers are beyond end of life and the vendor no longer supports that version of the operating system, thus the agency is no longer receiving security patches from the vendor. By not performing the vulnerability scans, and because servers do not have the latest critical security patches, the risk of successful cyber attacks significantly increases, which may cause the loss of data that may not be recovered.