U.S. Environmental Protection Agency
Office of Inspector General

13-P-0307
June 28, 2013

At a Glance

Why We Did This Review

This review was performed to assess the U.S. Chemical Safety and Hazard Investigation Board's compliance with the Federal Information Security Management Act of 2002.

FISMA requires federal agencies to develop an information security program that protects the operations and assets of the agency. An annual independent evaluation of the program must be performed by the inspector general or an independent external auditor, who shall report the results to the Office of Management and Budget. The U.S. Environmental Protection Agency, Office of Inspector General, which also serves as the Inspector General for the CSB, contracted with KPMG LLP to perform this fiscal year 2012 evaluation.

This report addresses the following CSB goal:

- *Preserve the public trust by maintaining and improving organizational excellence.*

For further information, contact our Office of Congressional and Public Affairs at (202) 566-2391.

The full report is at:
www.epa.gov/oig/reports/2013/20130628-13-P-0307.pdf

Evaluation of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (Fiscal Year 2012)

What KPMG Found

KPMG noted that the CSB has an information security program in place that appears to be functioning as designed. KPMG also noted that the CSB takes information security weaknesses seriously, as the CSB is performing vulnerability assessments on its network devices and security configuration assessments on a subset of its network devices. However, KPMG identified areas in which the CSB could improve upon its vulnerability scanning, patch and configuration management, device encryption, scanning software configuration, and inventory of IT assets.

In addition to reviewing the CSB's information security practices, KPMG conducted a security assessment of key CSB system and network devices. As a result of this assessment, KPMG found un-patched network devices and mobile devices that were not encrypted, which elevated the CSB's risk of system and data compromise by unauthorized users. KPMG also identified that the scanning tool used by the CSB for providing visibility into its network devices was not providing adequate visibility for its IT devices included within its physical inventory. KPMG also identified 130 personal computers for a staff of 44 members, six decommissioned Blackberries, two decommissioned servers, and 57 obsolete assets identified in the prior year audit that were not retired, which could allow for misuse or loss of IT devices or data.

KPMG is responsible for the content of the final audit report. The OIG performed the procedures necessary to obtain reasonable assurance about KPMG's independence, objectivity, qualifications, technical approach and audit results.

Recommendations and CSB Corrective Actions

KPMG recommends that the CSB take several actions to remediate the identified weaknesses. These include:

- Patching network devices and implementing baseline configurations.
- Implementing encryption on mobile assets and completing plans to implement tools for continuous monitoring of network devices.

The CSB agreed with the report's findings and recommendations. The CSB asserted that it was in the process of implementing the baseline configurations during the audit and will have the baseline configurations implemented by September 30, 2013. The CSB provided agreed-upon corrective actions for all the recommendations.