U.S. Environmental Protection Agency
Office of Inspector General

14-P-0181
April 10, 2014

At a Glance

Why We Did This Review

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

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's Office of Inspector General, which also serves as the Inspector General for the CSB, contracted with KPMG LLP to perform this fiscal year 2013 evaluation.

This report addresses the following CSB goal:

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

For further information, contact our public affairs office at (202) 566-2391.

The full report is at:
www.epa.gov/oig/reports/2014/20140410-14-P-0181.pdf

The U.S. Chemical Safety and Hazard Investigation Board Complies With the Federal Information Security Management Act (Fiscal Year 2013)

What KPMG Found

KPMG determined that the CSB has an information security program in place that appears to be functioning as designed. The CSB takes information security weaknesses seriously and is performing vulnerability assessments on its network devices and security configuration assessments on a subset of its network devices.

The CSB has an information security program in place that is functioning as designed; the CSB takes information security weaknesses seriously.

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

KPMG made no recommendations during this evaluation cycle. Evaluation work during this period disclosed that the CSB has taken sufficient actions to close all open recommendations noted during the fiscal year 2012 audit.

The CSB concurred with all report findings.

Noteworthy Achievements

During fiscal year 2013, the CSB implemented patching policy and procedures for its core network devices and computers. This included defining the associated baselines for these devices. The CSB also implemented the current version of its network security and patch management software, which allows greater insight into devices connected to the CSB general support system.