U.S. Environmental Protection Agency
Office of Inspector General

12-P-0363
March 21, 2012

At a Glance

Why We Did This Review

The review 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).

Background

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 CSB, contracted with KPMG LLP to perform the fiscal year 2011 evaluation.

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/2012/20120321-12-P-0363.pdf

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance With the Federal Information Security Management Act (Fiscal Year 2011)

What KPMG Found

KPMG noted that CSB has an information security program in place that appears to be functioning as designed. KPMG also noted that CSB takes information security weaknesses seriously, as three of the four prior-year recommendations were resolved. However, KPMG identified areas in which CSB could improve upon its vulnerability scanning and patch management process, and inventory of information technology assets.

In addition to reviewing CSB's information security practices, KPMG conducted a security assessment of key CSB system and network devices. This assessment disclosed several challenges CSB faces in securing its main information technology system. KPMG found unpatched network devices, which elevated CSB's risk of system and data compromise by unauthorized users. KPMG provided detailed results of its assessment to CSB officials. KPMG also identified 199 excess information technology devices, of a total of 408, which could allow for misuse or loss of information technology devices or data.

What KPMG Recommends

KPMG recommends that CSB review and implement patches for network devices as required, develop and implement standard baseline configurations for network devices, and review the information technology inventory and remove the excess inventory devices through appropriate means.

CSB agreed with the recommendations and provided agreed-upon corrective actions.