U.S. Environmental Protection Agency
Office of Inspector General

11-P-0148
March 8, 2011

At a Glance

Catalyst for Improving the Environment

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, Office of Inspector General, contracted with KPMG LLP to perform the fiscal year 2010 evaluation.

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

The full report is at:
www.epa.gov/oig/reports/2011/20110308-11-P-0148.pdf

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance With the Federal Information Security Management Act (Fiscal Year 2010)

What KPMG Found

KPMG noted that CSB does have an information security program in place that appears to be functioning as designed. KPMG also noted that CSB does take information security weaknesses seriously, as 8 of the 10 prior-year recommendations were resolved. However, KPMG identified areas in which CSB could improve upon its vulnerability scanning management process.

In addition to reviewing CSB's information security practices, KPMG conducted a security assessment of key CSB system and network devices. This assessment revealed several challenges CSB faces in securing its main information technology system. KPMG found insecure system protocols, default configuration settings, and unpatched network devices, which significantly elevated CSB's risk of system and data compromise by unauthorized users. KPMG provided detailed results of its assessment to CSB officials, and CSB worked proactively during the testing to address any identified high-risk issues.

What KPMG Recommends

KPMG recommends that CSB perform vulnerability scans and document audit log reviews consistently; implement baseline configurations for network devices; and develop, maintain, and test a contingency plan for the Information Technology System in accordance with National Institute of Standards and Technology guidance.

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