U.S. Environmental Protection Agency
Office of Inspector General

10-P-0174
August 2, 2010

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We performed this review 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

The U.S. Environmental Protection Agency (EPA) Office of Inspector General (OIG) contracted with KPMG, LLP, to perform the Fiscal Year (FY) 2009 FISMA assessment. The evaluation adhered to the Office of Management Budget (OMB) reporting guidance for microagencies, which CSB is considered. We also performed additional procedures to assess the information security program at CSB.

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

To view the full report, click on the following link:
www.epa.gov/oig/reports/2010/20100802-10-P-0174.pdf

Evaluation of the U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (Fiscal Year 2009)

What KPMG Found

During our FY 2009 evaluation, KPMG noted that CSB does have an information security program in place that appears to be functioning as designed. We also noted that CSB does take information security weaknesses seriously, as three of the four prior year issues were closed. However, during this year's assessment, we identified areas where CSB could improve upon its Risk Assessment, System Security Planning, Plans of Action and Milestones, Contingency Planning, Access Controls, and Audit Logging practices.

In addition to reviewing CSB's information security practices, KPMG conducted a network vulnerability test of key CSB system and network devices. This test revealed vulnerabilities related to insecure system protocols, default configurations, and unpatched devices. While Board Order 034 provides policies and procedures for maintaining device security, CSB personnel did not always follow this guidance to ensure that network devices were appropriately secured as prescribed. Insecure protocols, default configurations, and unpatched devices significantly elevate CSB's risk of system and data compromise by unauthorized users, which could lead to the alteration or deletion of critical data and a degradation of system performance. KPMG provided the network vulnerability results to CSB management and CSB worked diligently to remediate the identified weaknesses.

What KPMG Recommends

KPMG recommends that CSB:

- Provide appropriate training to CSB individuals responsible for completing the Information Technology System risk assessment, security plan, and access control procedures.
- Develop, maintain, and periodically test the Information Technology System contingency plan in accordance with Board Order 034 and federal guidance.
- Develop a process to maintain access approval requests for the Information Technology System.
- Update Board Order 034 to document a process for maintaining information security Plans of Action and Milestones.