U.S. Environmental Protection Agency
Office of Inspector General

2007-P-00019
April 23, 2007

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We sought to determine whether the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) information security program complies with the Federal Information Security Management Act (FISMA). We also sought to determine whether CSB complied with Office of Management and Budget (OMB) Memorandum M-06-16 requirements for protecting sensitive information.

Background

The Office of Inspector General (OIG) contracted with KPMG, LLP to assist in performing the Fiscal Year 2006 FISMA independent evaluation of the CSB information security program, and the Agency's efforts to protect its sensitive information. This evaluation adheres to the OMB reporting guidance for micro-agencies, which CSB is considered.

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

To view the full report, click on the following link:
www.epa.gov/oig/reports/2007/20070423-2007-P-00019.pdf

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act and Efforts to Protect Sensitive Agency Information (Fiscal Year 2006)

What KPMG Found

In Fiscal Year 2006, CSB made significant changes that enhanced the security of information system resources. CSB reorganized its Information Technology department by promoting and hiring key management officials. CSB also consolidated three information system functions into one Agency-owned General Support System (GSS) that mitigated a portion of the prior year weakness related to the implementation of security controls. The new GSS was certified and accredited for the operating environment. Further, CSB took steps to correct all of the security weaknesses identified during Fiscal Year 2005. However, KPMG found areas where CSB could further strengthen its information security program. KPMG found that:

- CSB's new consolidated GSS Security Plan did not address many of the Federal requirements prescribed by the National Institute of Standards and Technology. CSB also had not tested the new GSS' security controls for effectiveness. In addition, CSB had not assigned a risk categorization to the GSS in accordance with Federal requirements.
- While CSB reported a computer theft to the Federal Protective Service and the local police department, the incident was not reported to the United States Computer Emergency Readiness Team. Additionally, the theft was not documented in a formal incident report as required by CSB policy.
- CSB had not identified or implemented policies and procedures that address the protection of sensitive personally identifiable information.
- Although checklists are used to set up computers, there is no policy that mandates the use of the checklists, and the checklists did not contain security configuration settings. In addition, CSB had not developed an Agency-wide security configuration policy.
- CSB had not tested the GSS' contingency plan during Fiscal Year 2006 and the content of the plan needs improvement. Further, CSB had not conducted an e-authentication risk assessment.