U.S. Environmental Protection Agency
Office of Inspector General

2005-2-00030
September 28, 2005

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) information security program complies with the Federal Information Security Management Act (FISMA) for Fiscal Year 2005.

Background

The Office of Inspector General (OIG) contracted KPMG, LLP (KPMG) to assist in performing the Fiscal Year 2005 FISMA independent evaluation of the CSB information security program and practices. This evaluation adheres to the Office of Management and Budget 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/2005/20050928-2005-2-00030.pdf

Evaluation of U.S. Chemical Safety and Hazard Investigation Board's Compliance with the Federal Information Security Management Act (FISMA) for Fiscal Year 2005

What We Found

The U.S. Chemical Safety and Hazard Investigation Board (CSB) took significant actions to fill two critical vacancies. The appointments of the Chief Information Officer and the Information Technology Manager placed much needed attention on CSB's information security program. However, the 7- and 5-month delays in the respective appointments hampered CSB's ability to initiate actions to address significant deficiencies noted during the Fiscal Year 2004 Federal Information Security Management Act (FISMA) evaluation. Consequently, CSB did not remediate Fiscal Year 2004 weaknesses that are reported as repeat deficiencies in this year's evaluation. Although CSB has hired a contractor to assist them in correcting many of the identified weaknesses and created a timetable to alleviate their vulnerabilities, we found that CSB had not:

- Certified and accredited any of its information systems. In addition, CSB has not categorized its information systems in accordance with the National Institute of Standards and Technology (NIST) Federal Information Processing Standard 199, nor reviewed using security guidance contained in NIST Special Publications 800-26 and 800-53.

- Addressed long-standing weaknesses in implementing security controls such as completing risk assessments, implementing file and e-mail encryption, and establishing software patch management system. In addition, this year's evaluation identified that CSB needs to make improvements in testing its contingency plans, documenting security configuration standards, completing e-authentication risk assessments, testing security controls, and performing sufficient oversight for its contractor-operated system to ensure the system meets FISMA requirements.

- Approved its new security incident handling procedures, although some components of the procedures are in use.