08-P-0134
April 21, 2008

U.S. Environmental Protection Agency
Office of Inspector General

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 information security program compliance with the Federal Information Security Management Act (FISMA). Where appropriate, we also sought to make recommendations to ensure a security framework is in place that is capable of meeting security requirements into the future.

Background

CSB contracted with Total Systems Technologies Corporation (TSTC) to assist in performing the Fiscal Year 2007 FISMA assessment under the direction of the U.S. Environmental Protection Agency Office of Inspector General. The review adhered to the Office of Management and Budget reporting guidance for micro-agencies, which CSB is considered, and included an assessment of CSB progress in protecting its sensitive information, including Personally Identifiable Information.

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/2008/20080421-08-P-0134.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 2007)

What TSTC Found

During Fiscal Year 2007, CSB continued to make progress in improving the security of its information system resources. CSB had done this by performing the following:

- assigning a risk categorization to CSB's General Support System in accordance with Federal requirements,
- developing policies mandating the use of security configuration checklists and updating them to contain security configuration settings, and
- conducting contingency plan testing and an e-authentication risk assessment.

CSB has also taken the steps necessary to allow CSB management to align the organization's security program with the Personally Identifiable Information changes directed by the Office of Management and Budget. Further, CSB took the necessary steps to complete all but one of the planned actions in response to the security weaknesses identified during Fiscal Year 2006 audit.

What TSTC Recommends

TSTC did find areas where CSB could continue to improve its information security program. Specifically, TSTC recommends that CSB:

- Expand the security training to include specialized, role-based training.
- Document the CSB Breach Policy and related privacy information policies and procedures to meet CSB needs and Office of Management and Budget requirements.
- Update the CSB security policy and associated procedures to address reviewing, approving, and documenting non-standard security configurations.
- Update, as applicable, the appropriate security documentation to ensure compliance with National Institute of Standards and Technology Special Publication 800-53 controls guidance.