U.S. Environmental Protection Agency
Office of Inspector General

08-P-0295
September 29, 2008

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 of 2002 (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 2008 FISMA assessment under the direction of the U.S. Environmental Protection Agency (EPA) Office of the Inspector General (OIG). The review adhered to the Office of Management and Budget (OMB) 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/2008/20080929-08-P-0295.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 2008)

What TSTC Found

During Fiscal Year 2008, CSB continued to make significant progress in improving the security of its information system resources. CSB had done this by performing the following:

- Expanding the security training to include specialized, role-based training;
- Implementing incident response training and testing and issuing a Breach Policy; and
- Benchmarking and utilizing government and industry best practices and templates in updating the CSB Certification and Accreditation documentation, including the System Security Plan, the Risk Assessment, and the security test controls.

CSB has also taken the steps necessary to allow CSB management to align the organization's security program with the Personally Identifiable Information requirements issued by the OMB. CSB also took the necessary steps to complete six of the seven planned actions in response to the security weaknesses identified during the Fiscal Year 2007 audit. The remaining weakness regarding non-standard security configurations from the Fiscal Year 2007 audit is on schedule to meet the target completion date of October 10, 2008.

What TSTC Recommends

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

- Insert the approved security "banner" within all CSB database applications.
- Continue to update the CSB Configuration Management policy and associated procedures to address reviewing, approving, and documenting non-standard security configurations to meet the deadline established by CSB.
- Continue to update, as applicable, the appropriate security documentation to ensure compliance with National Institute of Standards and Technology Special Publication 800-53 controls guidance and update the security documents to include revision history information such as date of revision, individual who updated the document, and description of the revision.