U.S. Environmental Protection Agency
Office of Inspector General

2006-P-00019
March 28, 2006

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

As part of our annual audit of the Environmental Protection Agency's compliance with the Federal Information Security Management Act (FISMA), we reviewed the security practices for a sample of key Agency information systems, including the Comprehensive Environmental Response, Compensation, and Liability Information System (CERCLIS).

Background

FISMA requires agencies to develop policies and procedures commensurate with the risk and magnitude of harm resulting from the malicious or unintentional damage to the Agency's information assets. CERCLIS provides critical information in support of the Superfund program (a Federal mandate to clean up the Nation's uncontrolled hazardous waste sites).

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/2006/20060328-2006-P-00019.pdf

Information Security Series: Security Practices Comprehensive Environmental Response, Compensation, and Liability Information System

What We Found

The Office of Solid Waste and Emergency Response's (OSWER's) implemented practices to ensure production servers were being monitored for known vulnerabilities and personnel with significant security responsibility completed the Agency's recommended specialized security training. However, we found that OSWER's CERCLIS, a major application, was operating without a current (1) certification and accreditation package and (2) contingency plan or testing of the plan. OSWER officials could have discovered the noted deficiencies had they implemented practices to ensure these Federal and Agency information security requirements were followed. As a result, CERCLIS had security control weaknesses that could effect OSWER's operations, assets, and personnel.

What We Recommend

We recommend that the CERCLIS System Owner:

- Conduct an independent review of security controls and a full formal risk assessment of CERCLIS and update the certification and accreditation package in accordance with Federal and Agency requirements,
- Conduct a test of the updated CERCLIS contingency plan, and
- Develop a Plan of Action and Milestones in the Agency's security weakness tracking system (ASSERT database) for all noted deficiencies.

We recommend that the OSWER Information Security Officer:

- Conduct a review of OSWER's current information security oversight processes and implement identified process improvements.

OSWER agreed with the report's findings and has indicated that it has updated the CERCLIS security plan and re-authorized the application. OSWER officials also indicated that they updated the CERCLIS contingency plan and conducted a tabletop exercise of the updated plan. OSWER's complete response in included at Appendix A.