U.S. Environmental Protection Agency
Office of Inspector General

2006-P-00020
March 29, 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 Office of Enforcement and Compliance Assurance's (OECA's) Integrated Compliance Information System (ICIS).

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. ICIS provides critical data and processing in support of the Agency's environmental law enforcement and compliance program.

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/2006/20060329-2006-P-00020.pdf

Information Security Series: Security Practices Integrated Compliance Information System

What We Found

The Office of Enforcement and Compliance Assurance (OECA) had implemented practices to ensure that the (1) Integrated Compliance Information System (ICIS) production servers were monitored for known vulnerabilities and (2) personnel with significant security responsibility completed the Agency's recommended specialized security training. However, we found that OECA could improve its practices to ensure that key security documents are maintained. Additionally, ICIS, a major application, was operating without a contingency plan or testing of the plan. OECA officials could have discovered the noted deficiencies had they implemented processes to ensure these Federal and Agency information security requirements were followed. As a result, ICIS had security control weaknesses that could affect OECA's operations, assets, and individuals.

What We Recommend

We recommend that the ICIS System Owner:

- Conduct a review of processes used to maintain ICIS' key information security documents and implement identified process improvements,
- Conduct a test of the ICIS contingency plan, and
- Develop Plans of Action and Milestones (POA&Ms) in the Agency's security weakness tracking system (ASSERT database) for all noted deficiencies.

We recommend that the OECA Information Security Officer:

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

OECA agreed that ICIS needed a contingency plan and the office developed a plan. OECA did not agree that ICIS' security plan was not up-to-date, the office should create a plan to review its information security practices, and POA&Ms are needed for the identified weaknesses. Our audit disclosed that key security documents were not updated to reflect the results of critical security activities and although OECA developed a contingency plan, the office has not tested it. As such, OECA should re-evaluate its security oversight program to identify weaknesses and create POA&Ms to track remediation of uncompleted tasks. OECA's response is at Appendix A.