U.S. Environmental Protection Agency
Office of Inspector General

2006-P-00021
March 30, 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 (EPA'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 Water's (OW's) Safe Drinking Water Information System (SDWIS).

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. SDWIS supports EPA's initiative to protect public health by allowing EPA to provide a repository of national public drinking water data to interested stakeholders.

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/2006/20060330-2006-P-00021.pdf

Information Security Series: Security Practices Safe Drinking Water Information System

What We Found

We found that the Office of Water (OW) substantially complied with many of the information security controls reviewed and had implemented practices to ensure production servers are monitored for known vulnerabilities, physical access controls are adequate, and personnel with significant security responsibility completed the Agency's recommended specialized security training. However, we found that the Safe Drinking Water Information System (SDWIS), a major application, did not have complete certification and accreditation documents. In addition, the contingency plan did not contain all elements specified by Federal and Agency requirements. OW officials could have discovered the identified weaknesses had the office reviewed its implemented practices for completing these requirements. As a result, SDWIS had security control weaknesses that could affect OW's operations, assets, and individuals.

What We Recommend

We recommend that the SDWIS System Owner:

- Complete the independent review of security controls, complete a full formal risk assessment of SDWIS, and update the certification and accreditation package.
- Update and test the SDWIS contingency plan and implement a process to periodically test and maintain the plan.
- 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 OW Information Security Officer:

- Conduct a review of OW's information security oversight processes.

OW agreed with the report's findings, indicated that it was in the process of completing the risk assessment, and expected to complete the assessment by the end of March 2006. OW also stated it would update and test the SDWIS contingency plan as a follow-up to the formal risk assessment. OW expressed concerns that some of the findings could give a misleading picture of the security of SDWIS at the time of our review and we updated the report to reflect efforts OW took to address the findings. OW's complete response is in Appendix A.