U.S. Environmental Protection Agency
Office of Inspector General

2006-P-00024
May 4, 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 Air and Radiation's (OAR's) Clean Air Markets Division Business System (CAMDBS).

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. CAMDBS is the data system EPA uses to support the market-based emissions trading programs.

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/2006/20060504-2006-P-00024.pdf

Information Security Series: Security Practices Clean Air Markets Division Business System

What We Found

The Office of Air and Radiation (OAR) had substantially complied with many of the information security controls tested. In this regard, OAR developed and tested a contingency plan for the Clean Air Markets Division Business System (CAMDBS) and personnel with significant security responsibility completed the Agency's recommended specialized security training courses. However, our audit identified areas where OAR should place greater emphasis to comply with Federal and Agency information security requirements. We found that CAMDBS, a major application, was operating without (1) an up-to-date risk assessment and (2) effective practices to ensure that all production servers were monitored for known security vulnerabilities. OAR could have discovered the identified weaknesses had the office reviewed its implemented practices for completing these requirements as well as those of the National Computer Center (NCC), the group charged with primary responsibility for monitoring the servers. As a result, CAMDBS officials lacked key security management tools that could be used to proactively identify potential security weaknesses.

What We Recommend

We recommend that the CAMDBS System Owner:

- Conduct a full formal risk assessment of CAMDBS in accordance with Federal and Agency requirements.
- Coordinate with the NCC to verify that it is regularly monitoring all CAMDBS production servers for known vulnerabilities at least monthly.
- Develop a Plan of Action and Milestone in the Agency's information security weakness tracking system for all noted deficiencies.

We recommend that the OAR Information Security Officer:

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

OAR agreed with the findings in the draft report and indicated that the office has moved forward aggressively to implement the recommendations. OAR's complete response is in Appendix A.