U.S. Environmental Protection Agency
Office of Inspector General

2006-P-00010
January 31, 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 Administration and Resources Management's (OARM's) Integrated Contract Management System (ICMS).

## 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. ICMS is the information system EPA uses to manage its contracts.

**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/2006/20060131-2006-P-00010.pdf**

## *Information Security Series: Security Practices Integrated Contract Management System*

### What We Found

OARM should place greater emphasis on key information system security practices to comply with Federal and Agency information security requirements. Specifically, we found that OARM's ICMS, a major application, was operating without (1) current certification and accreditation, (2) contingency plans or testing of the plans, and (3) a process to monitor servers for known security vulnerabilities. OARM officials could have discovered these noted deficiencies had they implemented procedures to ensure that Federal and Agency information security policies and guidelines were followed. As a result, ICMS had security vulnerabilities, which, if exploited, could have had a serious adverse effect on operations, assets, and individuals.

### What We Recommend

We recommend that the OARM Information Security Officer:

- Develop a contingency plan for ICMS and implement a process to ensure the plan is tested at least annually,
- Implement processes to ensure ICMS production servers are periodically monitored for known vulnerabilities,
- Develop a Plan of Action and Milestone in the Agency's security weakness tracking system (ASSERT database) for all noted deficiencies, and
- Develop and implement a plan to re-evaluate system security oversight processes to ensure the above recommendations are uniformly applied to all general support systems and major applications within OARM.

OARM agreed with the report's findings and has indicated that the office has updated key security documents and started to address several of the identified issues. OARM maintains that the office has processes to ensure that ICMS servers it controls are monitored for known vulnerabilities. The office indicated many of the Office of Inspector General's concerns would be addressed when OARM finalizes its server consolidation project.