U.S. Environmental Protection Agency
Office of Inspector General

2006-P-00002
October 17, 2005

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

The Federal Information Security Management Act (FISMA) requires the Office of Inspector General to perform an independent evaluation of the Environmental Protection Agency's (EPA) information security program and practices.

Background

We selected a sample of the EPA's major applications and evaluated:

- certification and accreditation practices;
- system contingency plans; and
- program offices' processes to test and evaluate security controls, including conducting vulnerability tests for known security threats.

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/2006/20051017-2006-P-00002.pdf

EPA Could Improve Its Information Security by Strengthening Verification and Validation Processes

What We Found

Program offices had not effectively implemented processes to comply with Federal and EPA requirements related to information security. We found major applications without: (1) adequate certification and accreditation, (2) contingency plans or testing of the plans, and (3) a process to monitor for known security vulnerabilities. As such, all security control deficiencies are not reported in EPA's Plans of Action and Milestones system. EPA could have discovered these security deficiencies had it implemented processes to verify and validate offices' compliance with established Federal and Agency requirements. Therefore, the Chief Information Officer is not receiving timely and accurate information with which to plan, implement, evaluate, and report its Information Technology security status and security remediation activities to Office of Management and Budget.

What We Recommend

We made four recommendations to the Director of EPA's Office of Technology Operations and Planning. These involved: (1) developing and implementing an ongoing oversight process to review major applications and related general support systems for compliance with Federal and Agency requirements; (2) developing and implementing processes to evaluate the effectiveness of Independent Verification and Validation reviews; (3) developing a strategy for reporting Independent Verification and Validation results to inform Assistant and Regional Administrators on the status of their security programs; and (4) ensuring program offices establish Plans of Action and Milestones for all program office-specific deficiencies identified in subsequent reports related to this review.

The Agency found the report to be an accurate reflection of the Agency security program and concurred with the findings and recommendations.