U.S. Environmental Protection Agency
Office of Inspector General

2007-P-00007
January 11, 2007

At a Glance

Catalyst for Improving the Environment

Why We Did This Audit

We sought to determine whether the U.S. Environmental Protection Agency (EPA) defined security requirements for contractor-owned systems that collect data for EPA. We also sought to determine whether EPA offices identified and reported all computer security-related incidents to EPA's Computer Security Incident Response Capability (CSIRC) staff.

Background

EPA uses contractors to collect and process information on its behalf. Annually, the contractors review their systems' compliance with established information security requirements and record the results in EPA's security monitoring database. CSIRC defines the formal process by which EPA responds to computer security-related incidents such as computer viruses, unauthorized user activity, and serious software vulnerabilities.

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/2007/20070111-2007-P-00007.pdf

EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents

What We Found

Although EPA had defined the specific requirements for contractor systems, EPA had not established procedures to ensure identification of all contractor systems. Furthermore, EPA had not ensured that information security requirements were accessible by the contractors and appropriately maintained. As a result, EPA system inventories may not include all appropriate contractor systems, and its contractors may not be implementing adequate security safeguards.

Although EPA offices were aware of the Agency's computer security incident response policy, many offices lacked local reporting procedures, had not fully implemented automated monitoring tools, and did not provide sufficient training on local procedures. EPA offices also did not have access to network attack trend information necessary to implement proactive defensive measures. As a result, there was no consistency in how, what, and when EPA offices reported computer security incidents. Without all relevant security incident data, EPA may not accurately inform senior Agency officials regarding the performance and security of the Agency's network.

What We Recommend

To address weaknesses associated with contractor systems, we recommend that EPA assign duties and responsibilities for maintaining and updating information posted on EPA's Website. We also recommend that EPA update its guidance for identifying contractor systems. Further, we recommend that EPA establish formal procedures to ensure that all responsible program offices update and maintain their EPA-specific contract clauses on a regular basis.

To address the computer security incident reporting weaknesses, we recommend that EPA update the Agency's computer security incident guide to cover reporting instructions for all locations, establish a target date for when it will configure the Agency's anti-virus software to utilize the central reporting feature, train Information Security Officers on new procedures, and provide Information Security Officers with computer security incident reports.

The Agency generally agreed with our recommendations. In many cases, management provided milestone dates and planned actions to address the report's findings. The Agency's complete response is included at Appendices A and B.