U.S. Environmental Protection Agency
Office of Inspector General

11-P-0597
September 9, 2011

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

The U.S. Environmental Protection Agency (EPA), Office of Inspector General, conducted this audit to identify vulnerabilities associated with EPA's directory service system authentication and authorization servers, and provide the results to the appropriate EPA officials who can then promptly remediate and/or document planned actions to resolve the identified vulnerabilities. This audit was conducted in support of the audit of EPA's implementation of its directory service system.

Background

A directory service provides a centralized location to store information about the users, computers, and other equipment on a network, and provides integrated services that are used to manage network users, services, and devices. EPA uses a commercial-off-the-shelf product for its directory service system. This directory service system is implemented using multiple servers, which EPA has placed in various locations on its network to provide enterprise-wide authentication and authorization.

For further information, contact our Office of Congressional, Public Affairs and Management at (202) 566-2391.

Results of Technical Vulnerability Assessment: EPA's Directory Service System Authentication and Authorization Servers

What We Found

Vulnerability testing of EPA's directory service system authentication and authorization servers conducted in March 2011 identified authentication and authorization servers with numerous ***high-risk*** and ***medium-risk*** vulnerabilities. The Office of Inspector General met with EPA information security personnel to discuss the findings. If not resolved, these vulnerabilities could expose EPA's assets to unauthorized access and potentially harm the Agency's network.

What We Recommend

We recommend that the Director, Enterprise Desktop Services Division, Office of Environmental Information:

- Provide the Office of Inspector General a status update for all identified high-risk and medium-risk vulnerability findings contained in this report.
- Create plans of action and milestones in the Agency's Automated Security Self-Evaluation and Remediation Tracking system for all vulnerabilities that cannot be corrected within 30 days of this report.
- Perform a technical vulnerability assessment test of all Agency directory service system authentication and authorization servers within 60 days to confirm completion of remediation activities.

The full report is not available to the public due to the sensitive nature of its technical findings.