U.S. Environmental Protection Agency
Office of Inspector General

10-P-0210
September 7, 2010

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

As part of the annual audit of the U.S. Environmental Protection Agency's (EPA's) compliance with the Federal Information Security Management Act, the Office of Inspector General (OIG) conducted network vulnerability testing of the Agency's network devices in EPA's Andrew W. Breidenbach Environmental Research Center building located in Cincinnati, Ohio.

Background

Network vulnerability testing was conducted to identify any network risk vulnerabilities and to present the results to the appropriate EPA officials, who can then promptly remediate or document planned actions to resolve the vulnerability.

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

To view the full report, click on the following link:
www.epa.gov/oig/reports/2010/20100907-10-P-0210.pdf

Results of Technical Network Vulnerability Assessment: EPA's Andrew W. Breidenbach Environmental Research Center

What We Found

Vulnerability testing of EPA's Andrew W. Breidenbach Environmental Research Center network conducted in June 2010 identified Internet Protocol addresses with numerous ***high-risk*** and ***medium-risk*** vulnerabilities. The OIG 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 Senior Information Official, Office of Research and Development; Director, Enterprise Desktop Solutions Division, Office of Environmental Information; and Director, Information Resources Management Division – Cincinnati, Office of Administration and Resources Management:

- Provide the OIG 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 assigned network resources within 60 days to confirm completion of remediation activities.

Due to the sensitive nature of the report's technical findings, the attachments are not available to the public.