U.S. Environmental Protection Agency
Office of Inspector General

09-P-0055
December 9, 2008

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

The Office of Inspector General contracted with Williams, Adley & Company, LLP, to conduct the annual audit of the U.S. Environmental Protection Agency's (EPA's) compliance with the Federal Information Security Management Act (FISMA). Williams, Adley & Company, LLP, conducted the network vulnerability testing of the Agency's local area network located at EPA's National Computer Center in Research Triangle Park, North Carolina.

Background

The network vulnerability testing was conducted to identify any network risk vulnerabilities and present the results to the appropriate EPA officials to 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.

Results of Technical Network Vulnerability Assessment: EPA's National Computer Center

What Williams, Adley & Company, LLP, Found

Vulnerability testing of EPA's National Computer Center network identified Internet Protocol addresses with ***high-risk*** and ***medium-risk*** vulnerabilities. Although National Computer Center personnel have taken actions to remediate some of the documented findings, several vulnerabilities (both ***high*** and ***medium***) still remain unresolved.

What Williams, Adley & Company, LLP, Recommends

Williams, Adley & Company, LLP, recommends that the Director of the National Computer Center:

- Complete actions to address all unresolved vulnerability findings.
- Update EPA's Automated Security Self Evaluation and Remediation Tracking (ASSERT) system in accordance with the EPA Procedure for Information Security Plans of Actions and Milestones for the vulnerabilities not resolved within the required timeframes
- Perform a technical vulnerability assessment test of the National Computer Center network and managed assets at the Las Vegas Radiation and Indoor Environments National Laboratory, within 30 days, to demonstrate and document corrective actions that have resolved the vulnerabilities.

Due to the sensitive nature of this early warning report's technical findings, the full report is not available to the public.