U.S. Environmental Protection Agency
Office of Inspector General

09-P-0052
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 Region 9 office in San Francisco, California.

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: Region 9

What Williams, Adley & Company, LLP, Found

Vulnerability testing of EPA's Region 9 network identified Internet Protocol addresses with ***high-risk*** and ***medium-risk*** vulnerabilities. Although Region 9 has taken actions to remediate most of the documented findings, several vulnerabilities (both ***high*** and ***medium***) still remain resolved.

What Williams, Adley & Company, LLP, Recommends

Williams, Adley & Company, LLP, recommends that the Region 9 Director for Information Resources Management and Technical Services Division:

- Complete actions to address all unresolved vulnerability findings.
- Continue to work with the software vendor to resolve vulnerabilities. If the vendor is unable to provide a solution, implement a compensating control to resolve the risk.
- Enter a trouble ticket into EPA's REMEDY system to resolve the vulnerabilities associated with the Internet Protocol addresses under the National Computer Center's control.
- Update EPA's Automated Security Self Evaluation and Remediation Tracking (ASSERT) system.
- Perform a technical vulnerability assessment test of Region 9's network 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.