U.S. Environmental Protection Agency
Office of Inspector General

09-P-0188
June 30, 2009

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 network located at EPA's Potomac Yard buildings in Arlington, Virginia.

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 Potomac Yard Buildings

What Williams, Adley & Company, LLP, Found

Vulnerability testing of EPA's Potomac Yard buildings network conducted during April 2009 indicated several ***high-risk*** vulnerabilities. If not resolved, these vulnerabilities could expose EPA's assets to unauthorized access and potential harm to the Agency's network.

What Williams, Adley & Company, LLP, Recommends

There are four EPA offices involved with the Potomac Yard buildings: Office of Solid Waste and Emergency Response; Office of Prevention, Pesticides, and Toxic Substances; Office of Environmental Information; and Office of Research and Development. Williams, Adley & Company, LLP, recommends that the Acting Director, Office of Technology Operations and Planning, and the Senior Information Officials for these offices:

- Implement actions to resolve all high-risk vulnerability findings.
- Update EPA's Automated Security Self Evaluation and Remediation Tracking (ASSERT) system.
- Perform a technical vulnerability assessment within 30 days to demonstrate and document corrective actions have resolved the vulnerabilities.

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