



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 the EPA Research Triangle Park Campus in 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 Research Triangle Park Campus

What Williams, Adley & Company, LLP, Found

Vulnerability testing of EPA's Research Triangle Park Campus network identified Internet Protocol addresses with *high-risk* and *medium-risk* vulnerabilities. The National Computer Center (NCC) personnel have taken actions to remediate the majority of the documented findings. However, several vulnerabilities (both *high* and *medium risk*) still remain unresolved on information technology assets outside the control of the NCC.

On December 9, 2008, we issued this report to NCC outlining several weaknesses that remained uncorrected since issuing the draft vulnerability assessment report. NCC provided an updated status to address the weaknesses under their control, and upon further discussion we learned that several weaknesses must be corrected by other organizations within the Research Triangle Park Campus. We reissued this report to make further distribution of the vulnerability test results to other responsible organizations within the Research Triangle Park Campus.

What Williams, Adley & Company, LLP, Recommends

Williams, Adley & Company, LLP, recommends that the Directors for the Office of Information Resources Management Division, Office of Administration and Resources Management at Research Triangle Park and the Office Director, Office of Scientific Information Management, Office of Research and Development:

- 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 their Research Triangle Park Campus network assets to demonstrate that corrective actions 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.