U.S. Environmental Protection Agency
Office of Inspector General

12-P-0900
September 27, 2012

At a Glance

Why We Did This Review

We sought to conduct network vulnerability testing of the U.S. Environmental Protection Agency's (EPA's) National Vehicle and Fuel Emissions Laboratory (NVFEL) Local Area Network to identify resources that contained commonly known ***high-risk*** and ***medium-risk*** vulnerabilities. We also sought to assess the physical controls and environmental controls around critical information technology assets located in the NVFEL. We conducted this audit as part of the annual review of EPA's information security program as required by the Federal Information Security Management Act.

This report addresses the following EPA Goal or Cross-Cutting Strategy:

- *Strengthening EPA's Workforce and Capabilities*

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

The full report is at:
www.epa.gov/oig/reports/2012/20120927-12-P-0900.pdf

Results of Technical Network Vulnerability Assessment: EPA's National Vehicle and Fuel Emissions Laboratory

What We Found

While our assessments of EPA's NVFEL server room found no weaknesses with physical controls and environmental controls, vulnerability testing of networked resources located in the NVFEL identified Internet Protocol addresses with potentially 9 ***critical-risk***, 70 ***high-risk,*** and 297 ***medium-risk*** vulnerabilities. If not resolved, these vulnerabilities could expose EPA's assets to unauthorized access and potentially harm the Agency's network. The laboratory and the Office of Environmental Information manage the resources located in NVFEL that contained these weaknesses. We found a discrepancy between the offices concerning responsibility for certain equipment located in the NVFEL. However, NVFEL provided documentation which placed ownership responsibility with the Office of Environmental Information and Customer Technology Solutions for the devices in question.

Recommendations and Agency Corrective Actions

We recommend that the Senior Information Official within the Office of Air and Radiation and the Office of Environmental Information:

- Provide the OIG a status update for every critical-risk, high-risk and medium-risk vulnerability identified by the technical scanning tool within 30 days of this report.
- Create plans of action and milestones in the Agency's Automated Security Self-Evaluation and Remediation Tracking system for all vulnerabilities according to Agency procedures within 30 days of this report.
- Perform a technical vulnerability assessment test of assigned networked resources within 60 days to confirm completion of remediation activities.

We also recommend that the Senior Information Official within the Office of Environmental Information:

- Disconnect any networked resources without documented ownership responsibility.
- Complete an inventory of all Customer Technology Solutions equipment prior to implementation of EPA's new managed desktop support system.

Representatives from both offices acknowledged the existence of the vulnerabilities and stated they have begun developing corrective actions to address the risks related to these weaknesses. NVFEL reported it remediated all high-risk vulnerabilities under its responsibility prior to the issuance of this report.

The detailed testing results have already been provided to Agency representatives. Due to the sensitive nature of the report's technical findings, the technical details will not be made available to the public.