U.S. Environmental Protection Agency
Office of Inspector General

12-P-0518
June 5, 2012

At a Glance

Why We Did This Review

We sought to assess the security configurations of the U.S. Environmental Protection Agency's (EPA's) Region 1 wireless network infrastructure. We also sought to conduct network vulnerability testing of the Region 1 Local Area Network to identify resources that contained commonly known ***high-risk*** and ***medium-risk*** vulnerabilities.

Background

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. We conducted network vulnerability testing in February 2012 to identify any commonly known network vulnerabilities and to present the results to the appropriate EPA officials, who can then promptly remediate or document planned actions to resolve the weaknesses.

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/2012/20120605-12-P-0518.pdf

Results of Technical Network Vulnerability Assessment: EPA's Region 1

What We Found

Our vulnerability assessments of Region 1's wireless network infrastructure found no security weaknesses. However, our vulnerability testing of networked resources located at the Region 1 facility identified Internet Protocol addresses with potentially 18 ***high-risk*** and 166 ***medium-risk*** vulnerabilities. Regional and headquarter offices manage resources located in Region 1 that contain these weaknesses. The Office of Inspector General (OIG) met with EPA information security personnel from the respective offices to discuss the findings. EPA information security personnel acknowledged the existence of the identified security weaknesses and began immediate remediation of some of these issues. If not resolved, these vulnerabilities could expose EPA's assets to unauthorized access and potentially harm the Agency's network.

What We Recommend

We recommend that the Senior Information Officials within Region 1 and the Office of Environmental Information:

- Provide the OIG a status update for all identified high-risk and medium-risk vulnerability findings 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 network resources within 60 days to confirm completion of remediation activities.

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.

Planned Agency Corrective Actions

Region 1 remediated all high-risk vulnerabilities discovered by our vulnerability testing of networked resources. Additionally, Region 1 acknowledged the existence of the additional vulnerabilities that we identified and began mitigation activities related to these risks.