U.S. Environmental Protection Agency
Office of Inspector General

12-P-0659
August 10, 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 6 wireless network infrastructure. We sought to conduct network vulnerability testing of the Region 6 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 Region 6. 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.

Furthering EPA's Goals and Cross-Cutting Strategies

- *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/2012/20120810-12-P-0659.pdf

Results of Technical Network Vulnerability Assessment: EPA's Region 6

What We Found

Our vulnerability assessments of EPA's Region 6 wireless network infrastructure found no security weaknesses. However, our vulnerability testing of networked resources located at Region 6 facilities identified Internet Protocol addresses with potentially 35 ***critical-risk***, 217 ***high-risk,*** and 878 ***medium-risk*** vulnerabilities. Additionally, our server room assessments revealed a lack of adequate monitoring of environmental controls, the lack of a process to ensure only authorized personnel are approved for access to server rooms, and the existence of unsecured and unlogged media in the server rooms. If not resolved, these vulnerabilities could expose EPA's assets to unauthorized access and potentially harm the Agency's network.

Recommendations and Agency Corrective Actions

We recommend that the Senior Information Official within Region 6 provide the Office of Inspector General a status update for every critical-risk, high-risk, and medium-risk vulnerability identified by the scanning tool; create plans of action and milestones in the Agency's Automated Security Self-Evaluation and Remediation Tracking system for all vulnerabilities according to Agency interim procedures; perform a technical vulnerability assessment test of assigned network resources within 60 days to confirm completion of remediation activities; and remediate all identified physical and environmental control weaknesses identified in the server rooms.

Region 6 representatives acknowledged the existence of the vulnerabilities that we identified and stated they have begun developing corrective actions to address the risks related to these weaknesses.

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.