At a Glance

Why We Did This Review

The U.S. Environmental Protection Agency (EPA) Office of Inspector General (OIG) conducted this audit to identify technical vulnerabilities associated with the Agency's network devices located in EPA's Region 10 headquarters building, and to assess the security posture of the Region 10 computer room. Results of this audit were provided to the appropriate EPA officials who can then promptly remediate and/or document their planned actions to resolve the identified technical vulnerabilities and computer room security findings.

Background

This audit was conducted in support of the annual audit of EPA's compliance with the Federal Information Security Management Act.

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/
20120120-12-P-0220.pdf**

Region 10 Technical and Computer Room Security Vulnerabilities Increase Risk to EPA's Network

What We Found

OIG technical vulnerability scans conducted at Region 10 headquarters revealed a multitude of *high-risk* and *medium-risk* vulnerabilities. These vulnerabilities were identified on Region 10 servers, printers, and/or desktops. The exploitation of unidentified and unremediated vulnerabilities could greatly impact the network security posture of Region 10 headquarters and/or the entire EPA network by exposing Agency data, information, and configurations to unauthorized access.

The OIG physical and environmental control review of the Region 10 computer room found that sufficient protections were not in place to safeguard critical information technology assets and associated data from the risk of damage and/or loss.

What We Recommend

We recommend that the Senior Information Official, Region 10:

- Remediate high-risk and medium-risk technical vulnerabilities
- Remediate physical and environmental control deficiencies

The full report is not available to the public due to the sensitive nature of its technical findings.