U.S. Environmental Protection Agency
Office of Inspector General

2005-P-00011
March 22, 2005

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We sought to determine whether the Environmental Protection Agency's (EPA's) remote access methods, particularly through Web-Mail servers and BlackBerry servers and devices, have adequate controls to prevent abuse or unauthorized access to the Agency's information resources.

Background

Remote access is the connecting to EPA's data communications network from alternate locations not directly connected to the network. EPA establishes the security policy for the national data communications network and basic controls to ensure a secure infrastructure. Two key methods of attaining remote access are through an internet browser via Web-Mail or through a BlackBerry, which is a wireless handheld device.

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

To view the full report, click on the following link:

www.epa.gov/oig/reports/2005/20050322-2005-P-00011.pdf

Security Configuration and Monitoring of EPA's Remote Access Methods Need Improvement

What We Found

System administrators did not configure EPA's Web-Mail and BlackBerry servers to provide secure remote access to the Agency's network. We found that the system administrators did not configure or update 59 percent of the Web-Mail and BlackBerry servers to mitigate vulnerabilities. Consequently, confidentiality and integrity of EPA data, as well as the availability of the network, is at risk of unintentional or intentional exploitation. The weaknesses occurred because management did not implement processes to exercise proper oversight and provide detailed configuration settings.

We also found several of the Agency's BlackBerry devices were not adequately configured, secured, or monitored. We found devices that had no password enabled or had functionality that would allow users to disable passwords. We also observed devices left unattended in workstation cubicles. An unauthorized user of an unprotected handheld device has the potential to negatively affect the integrity and confidentiality of EPA information. These weaknesses occurred because management did not conduct a risk assessment or establish a process to consistently install BlackBerry devices.

What We Recommend

We made seven recommendations to the Director of EPA's Office of Technology Operations and Planning. They included establishing and requiring all remote access systems to have security monitoring and network vulnerability scanning; developing standards that define authorized open ports and services for the Web-Mail and BlackBerry servers' Operating System; and conducting a risk assessment and establishing a process to consistently configure devices. The Agency generally agreed with the recommendations and indicated corrective actions that, when implemented, would address the recommendations.