U.S. Environmental Protection Agency
Office of Inspector General

13-P-0252
May 8, 2013

At a Glance

Why We Did This Review

We sought to determine to what extent management at U.S. Environmental Protection Agency-owned research facilities establish and implement information security practices to protect Agency information technology assets. Agency IT assets must be maintained in accordance with security requirements defined by applicable federal laws, executive orders, directives, policies, standards, and regulations to ensure adequate confidentiality, availability, and integrity of the resources and information stored on or transmitted through the EPA network. Network vulnerabilities can expose IT assets to significant risk and disrupt operations if not identified and resolved.

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/2013/20130508-13-P-0252.pdf

Improvements Needed to Secure IT Assets at EPA-Owned Research Facilities

What We Found

Facilities management at the Office of Research and Development facilities does not consistently apply, or in some cases establish, controls to protect IT assets. We found instances where IT security practices at the facilities did not meet minimal recommended controls for securing IT assets. Chief among our findings are the following:

- IT equipment was unprotected from and unmonitored for water damage.
- Access to server rooms was unrestricted.
- No continuity of operations plan exists for provisioning IT equipment.
- Backup data were not stored offsite.

The National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* among other federal and Agency policies and procedures, provides minimum security-control recommendations. Many security weaknesses occurred at ORD facilities because these facilities did not follow federal and Agency guidance that prescribes measures for securing IT assets. Further, ORD facilities did not consistently perform or, when necessary, enhance security practices established to protect their facilities, as well as the IT resources within their custody. Failure to consistently follow, perform, and monitor recommended and established security practices compromises the security of IT assets, disrupts business operations, and exposes sensitive Agency information.

Recommendations and Planned Agency Corrective Actions

Management agreed with 14 of the 18 report recommendations to improve practices at ORD facilities. We consider these recommendations unresolved until the Agency provides planned completion dates. Management did not agree with recommendations to improve controls around the closed-circuit television system and to protect servers from accidental water damage. These recommendations are unresolved. We believe it is incumbent upon management to assess the risks for not implementing these needed measures. Furthermore, when required by federal guidance, management should document its decisions and have the responsible official formally accept responsibility.

Noteworthy Achievements

We conducted tests to determine the effectiveness of security practices for remote-access capability. We concluded that ORD labs implemented effective IT security controls that prevent unauthorized connection and communication by limiting access to the Agency's network through wireless network-access points.