U.S. Environmental Protection Agency
Office of Inspector General

12-P-0899
September 27, 2012

At a Glance

Why We Did This Review

The U.S. Environmental Protection Agency (EPA) Office of Inspector General (OIG) conducted this audit to (1) identify which tools EPA uses to identify, analyze, and resolve cyber-security incidents; (2) identify steps implemented to resolve known weaknesses in its incidence response capabilities; and (3) evaluate how users report security incidents.

Continually monitoring network threats through intrusion detection and prevention systems and other mechanisms is essential. Establishing clear procedures for assessing the current and potential business impact of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data.

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/2012/20120927-12-P-0899.pdf

Improvements Needed in EPA's Network Security Monitoring Program

What We Found

EPA's deployment of a Security Incident and Event Management (SIEM) tool did not comply with EPA's system life cycle management procedures, which require planning project activities to include resources needed, schedules, and structured training sessions. EPA did not develop a comprehensive deployment strategy for the SIEM tool to incorporate all of EPA's offices or a formal training program on how to use the tool. When EPA staff are not able to use an information technology investment, the investment has limited value in meeting organizational goals and users' needs.

EPA does not have a computer security log management policy consistent with federal requirements. While EPA has a policy governing minimum system auditing activities to be logged, EPA has yet to define a policy for audit log storage and disposal requirements along with log management roles and responsibilities. EPA risks not having logged data available when needed, and program officials may not implement needed security controls.

EPA did not follow up with staff to confirm whether corrective actions were taken to address known information security weaknesses. EPA had not taken steps to address weaknesses identified from internal reviews as required. Known vulnerabilities that remain unremediated could leave EPA's information and assets exposed to unauthorized access.

Recommendations and Planned Agency Corrective Actions

We recommended that the Assistant Administrator for Environmental Information develop and implement a strategy to incorporate EPA's headquarters program offices within the SIEM environment, develop and implement a formal training program for the SIEM tool, develop a policy or revise the Agency's Information Security Policy to comply with audit logging requirements, and appoint a central point of contact to track remediation of internal assessment weaknesses.

Office of Environmental Information officials concurred with and agreed to take corrective actions to address all recommendations.

Noteworthy Achievements

We found that EPA employees are aware of the reporting procedures for when they experience an information security incident. Additionally, EPA has recently deployed technical tools to combat cyber-security attacks and conduct forensic analyses of security activity.