U.S. Environmental Protection Agency
Office of Inspector General

11-P-0159
March 14, 2011

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We sought to determine whether the U.S. Environmental Protection Agency (EPA) is effectively managing Agency resources by implementing a management control structure to monitor internal and external computer network traffic.

Background

EPA spends approximately $160 million annually to support Agency network operations and infrastructure. We believe this sum reflects the importance placed on Internet connectivity and the degree to which Agency operations are now conducted electronically. As new threats associated with the electronic exchange of information emerge, information security has become a greater concern. Recent information technology audits continue to identify weaknesses in the Agency's information technology security program and information systems.

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

Improvements Needed in EPA's Network Traffic Management Practices

What We Found

The Office of Environmental Information (OEI) does not have consistent, repeatable intrusion detection system monitoring practices in place, which inhibits EPA's ability to monitor unusual network activity and thus protect Agency systems and associated data. OEI also has not documented a methodology to aid in making decisions about potentially unusual network traffic. The Federal Information Security Management Act requires each agency head to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of Agency information systems. Additionally, the act states that the National Institute of Standards and Technology shall prescribe standards and guidelines pertaining to federal information systems. Agency network security program deficiencies greatly decrease the likelihood that consistent, repeatable results are produced in identifying threats to the Agency's network and increase the likelihood that potential threats will not be identified.

OEI does not consistently conduct management oversight of contractor performance and reporting. In addition, key federally required security documents for EPA's Wide Area Network (WAN) were not complete or accurate. Furthermore, the approved security plan had not been updated to reflect the current infrastructure and an associated authorization to operate was not issued prior to implementing the secondary Internet connection. Office of Management and Budget Circular A-123 outlines management's responsibilities for establishing controls and performing oversight to ensure activities are performed as management intends. The Agency cannot accurately depict the operating environment and implement a system that meets federal requirements unless it can ensure that the security plan is complete, accurate, and approved.

What We Recommend

We recommend that the Director, Office of Technology Operations and Planning, Office of Environmental Information, develop and implement comprehensive log review policies and procedures, establish a management control process to review contractor performance, and update and approve the WAN security plan and properly certify and accredit future significant WAN configuration changes prior to moving them into production. The Agency agreed with our recommendations.

Due to the sensitive nature of the report's technical findings, the full report is not available to the public.