



At a Glance

Catalyst for Improving the Environment

Why We Did This Review

The Office of Inspector General (OIG) sought to determine (1) the status of corrective actions related to agreed-to recommendations for selected information security audit reports, and (2) to what extent the U.S. Environmental Protection Agency (EPA) program offices evaluated whether corrective actions taken resolved identified weaknesses.

Background

Office of Management and Budget (OMB) Circular A-123 requires that EPA managers take timely and effective action to correct deficiencies identified by a variety of sources, such as OIG audits. OMB Circular A-123 also requires management to show that corrective actions taken achieve the desired results. EPA Manual 2750 and EPA Order 1000.24 outline management's responsibility for following up on OIG recommendations.

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

To view the full report, click on the following link:
www.epa.gov/oig/reports/2009/20090921-09-P-0240.pdf

Project Delays Prevent EPA from Implementing an Agency-wide Information Security Vulnerability Management Program

What We Found

EPA implemented 56 percent (15 of 27) of the information security audit recommendations we reviewed. EPA's lack of progress on four key audit recommendations we made in 2004 and 2005 inhibits EPA from providing an Agency-wide process for security monitoring of its computer network. EPA has not established an Agency-wide network security monitoring program because EPA did not take alternative action when this project ran into significant delays. By not performing this critical function, EPA management lacked information necessary to respond to known threats against EPA's network and to mitigate vulnerabilities before they can be exploited.

EPA offices do not regularly evaluate the effectiveness of actions taken to correct identified deficiencies, as required by OMB Circular A-123. EPA is updating its audit management and oversight policies; we provided suggestions for strengthening them.

What We Recommend

We recommend that the Director of the Office of Technology Operations and Planning, within the Office of Environmental Information:

- Create Plans of Action and Milestones for each unimplemented audit recommendation listed in Appendix B.
- Update EPA's Management Audit Tracking System to show the status of each unimplemented audit recommendation listed in Appendix B.
- Provide EPA program and regional offices with an alternative solution for vulnerability management, including establishing a centralized oversight process to ensure that EPA program and regional offices (a) regularly test their computer networks for vulnerabilities, and (b) maintain files documenting the mitigation of detected vulnerabilities.
- Establish a workgroup of program and regional EPA information technology staff to solicit input on training needs and facilitate rolling out the Agency-wide vulnerability management program.
- Issue an updated memorandum discussing guidance and requirements.

The Agency agreed with all of our findings and recommendations.