U.S. Environmental Protection Agency
Office of Inspector General

10-P-0028
November 16, 2009

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) implemented oversight practices for the Customer Technology Solutions (CTS) contract. We are continuing our review and plan to issue a separate report on whether EPA has responded to resolve issues identified during CTS deployment, and implemented processes to eliminate recurring problems with deploying CTS.

Background

EPA indicates CTS is the Agency's Working Capital Fund service, providing and coordinating all information technology end user support and services for Headquarters program offices. EPA plans for CTS to be a one-stop shop for personal computing and information technology support services. EPA will deploy CTS equipment at 18 locations across the United States.

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/2010/20091116-10-P-0028.pdf

Improved Security Planning Needed for the Customer Technology Solutions Project

What We Found

EPA lacks a process to routinely test CTS equipment for known vulnerabilities and to correct identified threats. Furthermore, EPA placed CTS equipment into production without fully assessing the risk the equipment poses to the Agency's network and authorizing the equipment for operations. The Office of Management and Budget requires federal agencies to create a security plan for each general support system and ensure the plan complies with guidance issued by the National Institute of Standards and Technology. Both vulnerability management and the preparation of critical security documents such as the Security Plan and the Authorization to Operate are paramount to fulfilling this requirement. These weaknesses exist because EPA undertook an aggressive schedule to install over 11,500 computers at 18 locations across the United States. As problems occurred during installation, management focused its attention on addressing these issues in order to meet the deployment schedule milestone.

Given the widespread use of CTS equipment, thousands of information resources provide a path for potential unauthorized access to EPA's network. EPA lacks processes to identify these threats or the capability to lessen their impact.

On November 9, 2009, management signed an authorization to operate for the CTS equipment and outlined key actions that needed to be completed.

What We Recommend

We recommend that the Director, Office of Technology Operations and Planning and Chief Technology Officer, Office of Environmental Information, direct the CTS contractor to develop and implement a vulnerability testing and remediation process for CTS equipment consistent with existing EPA security policies and procedures, and issue a memorandum to Agency Senior Information Officials requiring their program office to conduct vulnerability testing of CTS equipment until a formal vulnerability testing and management process with CTS has been established.

Until this process is in place, we further recommend that the Director require the CTS contractor to remediate identified vulnerabilities in a timely manner and inform the respective Senior Information Official when they complete the corrective actions necessary to fix the vulnerabilities. We also recommend the Director ensure all key actions outlined in the November 9, 2009, CTS authorization to operate are completed by the defined milestone dates.