U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Quick Reaction Report

Improved Security Planning Needed for the Customer Technology Solutions Project

Report No. 10-P-0028

November 16, 2009

Report Contributors: Rudolph M. Brevard
Vincent Campbell
Charles M. Dade
Cheryl Reid

Abbreviations

ASSERT	Automated System Security Evaluation and Remediation Tracking
CTS	Customer Technology Solutions
EPA	U.S. Environmental Protection Agency
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget

Cover photo: Standard Customer Technology Solutions laptop used by EPA employees. (EPA photo)

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.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

November 16, 2009

MEMORANDUM

SUBJECT: Improved Security Planning Needed for the
Customer Technology Solutions Project
Report No. 10-P-0028

FROM: Rudolph M. Brevard
Director, Information Resources Management Assessments

TO: Vaughn Noga
Acting Director, Office of Technology Operations and Planning and
Chief Technology Officer, Office of Environmental Information

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The estimated cost of this report – calculated by multiplying the project's staff days by the applicable daily full cost billing rates in effect at the time – is $271,418.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to this report within 90 calendar days. You should include a corrective actions plan for agreed-upon actions, including milestone dates. We have no objections to the further release of this report to the public. This report will be available at http://www.epa.gov/oig.

If you or your staff have any questions regarding this report, please contact me at (202) 566-0893 or brevard.rudy@epa.gov; or Cheryl Reid, Project Manager, at (919) 541-2256 or reid.cheryl@epa.gov.

Table of Contents

Appendix

Purpose

The Office of Inspector General (OIG) sought to determine whether the U.S. Environmental Protection Agency (EPA) implemented oversight practices for the Customer Technology Solutions (CTS) contract.

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 single stop for personal computing and information technology support services. As shown on the map at right, EPA will place CTS equipment in 18 locations across the United States.

Source: EPA Office of Environmental Information Intranet

Scope and Methodology

We performed this audit from April 2009 through October 2009 at EPA Headquarters in Washington, DC, and the National Computer Center in Durham, North Carolina. We also visited the Headquarters field offices located in Las Vegas, Nevada, and the following EPA laboratories:

- National Exposure Research Laboratory in Athens, Georgia
- National Air and Radiation Laboratory in Montgomery, Alabama
- National Vehicle and Fuel Emissions Laboratory in Ann Arbor, Michigan

We performed this audit in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions.

We reviewed the CTS statement of work and interviewed EPA and contractor personnel responsible for overseeing the CTS project. We also spoke with EPA Program Office officials using the CTS equipment and EPA security personnel responsible for responding to security incidents for their respective offices.

We had not performed past audits of CTS. We did however, issue a report related to vulnerability management entitled *Project Delays Prevent EPA from Implementing an Agency-wide Information Security Vulnerability Management Program*, Report No. 09-P-0240, September 21, 2009.

Findings

EPA lacks a process to routinely test CTS computers for known vulnerabilities and a defined structure to remediate them. These weaknesses exist because EPA did not specify, in the CTS statement of work, that the CTS contractor was to perform vulnerability management. EPA installed CTS equipment without assessing the risks to the Agency's network and without authorizing the equipment for operations. Appendix III to Office of Management and Budget (OMB) Circular A-130, *Security of Federal Automated Information Resources*, requires federal agencies to create a security plan for each general support system. OMB also requires the plan to comply with guidance issued by the National Institute of Standards and Technology (NIST). Both vulnerability management and the preparation of critical security documents such as the Security Plan and the Authorization to Operate are necessary to meet this requirement.

EPA officials indicated the CTS equipment did not have all required security documents because EPA officials rejected the contractors' initial security plan. EPA officials indicated meeting this requirement became a lower priority due to the aggressive schedule the Agency was under for deploying the CTS equipment. As such, management lacks information it needs to protect the Agency's network from possible threats posed by the CTS equipment. Given the widespread use of CTS equipment in EPA, thousands of unmonitored assets reside on the Agency's network. The unmonitored assets could potentially provide a path for someone to obtain unauthorized access to the Agency's network. Without taking action, EPA's network remains exposed to possible threats without a process to identify them or the means to lessen their impact in a timely manner.

CTS Project Lacks a Process to Identify and Remediate Known Vulnerabilities

EPA does not have a process in place to test CTS equipment for known vulnerabilities. Based on discussions with both EPA and CTS contractor staff, none of the personnel knew whether there was a process in place. In addition, all indicated that this task was not being performed. Review of the CTS statement of work disclosed that vulnerability testing was not part of the CTS team's responsibility.

During our annual review of EPA's information security program, OIG contractors conducted network vulnerability testing of EPA Headquarters program office networks and identified several high-risk vulnerabilities. Summary results of these tests are posted on the OIG's Website. Upon analysis of these network tests, EPA system owners stated they do not have the capability to fix the vulnerabilities. System owners stated they do not have system administration rights for CTS equipment. Therefore, they are unable to remediate the high-risk vulnerabilities. System owners also indicated they are not aware of the process to mitigate vulnerabilities for CTS equipment connected to the Agency's network. They also stated that they do not know who is responsible for conducting the assessments and correcting known vulnerabilities for CTS equipment.

NIST Special Publication 800-123, *Guide to General Server Security*, states that vulnerability testing should occur on a weekly to monthly basis. NIST stresses that this ongoing testing is

extremely important for mitigating vulnerabilities as soon as possible to prevent them from being discovered and exploited. EPA requires the CTS contractor to use the Agency's tool that checks systems for correct configuration settings. However, this tool does not have the means to detect and provide solutions to remediate commonly known security vulnerabilities.

Compounding this issue, EPA has not made progress on four key audit recommendations we made in 2004 and 2005.[1] This lack of progress inhibits EPA from providing an Agency-wide process for security monitoring of its computer network. Given the widespread use of CTS computers throughout EPA and the fact that EPA does not have its own vulnerability management program, EPA has hampered its ability to know what threats exists on its network.

CTS Project Lacks Required Security Planning

EPA had not taken steps to fully assess the threats CTS equipment pose to the Agency's network. Fundamental to the assessment is preparing a Security Plan. The purpose of the system Security Plan is to provide an overview of the security requirements of the system and to describe the controls in place or planned for meeting those requirements. The Security Plan outlines responsibilities and expected behavior of all individuals who access the system. The main component in having an approved Security Plan is certifying the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome. This certification process results in an EPA official formally authorizing a system to operate.

OMB Guidance on Security of Federal Automated Information Resources	
System Security Plan	Plan for adequate security of each general support system as part of the organization's information resources management planning process.
Authorize Processing	Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system.

Source: OIG extract from OMB Circular A-130

OMB Circular A-130 requires agencies to establish a minimum set of controls to be included in federal automated information security programs. OMB further cites the Security Plan, Authorization to Operate, and incident handling as critical components. Likewise, OMB indicates, depending on the potential risk and magnitude of harm that could occur, management should consider identifying a deficiency pursuant to OMB Circular A-123, *Management Accountability and Control*. OMB also indicates that management should report, under the Federal Managers' Financial Integrity Act, if there is no Security Plan or no Authorization to Operate.

Headquarters' offices replaced their equipment with equipment provided by the CTS contractor. Therefore, the offices did not feel they had responsibility for monitoring the security of this equipment. Program office officials indicated the Agency had not established roles of responsibilities agreements with their offices. Therefore, they are not sure what role they play in protecting the Agency's network when it comes to CTS equipment. Furthermore, without defined roles and responsibilities it would be difficult for them to answer questions related to

[1] EPA–OIG. *Project Delays Prevent EPA from Implementing an Agency-wide Information Security Vulnerability Management Program.* Report No. 09-P-0240, September 21, 2009.

CTS equipment certification and accreditation, system inventory, or contractor oversight. EPA management indicated it rejected the initial Security Plan submitted by the CTS contractor. Management cited that this led to no security plan being in place for the CTS equipment. Management indicated that the rejected Security Plan lacked the specific details that were required by NIST. Management indicated that due to the time schedule for deploying the CTS equipment, completing the security documentation became a lower priority.

Management showed us a draft security plan they planned to send through their office's quality assurance process. Management indicated the CTS contractor also conducted network vulnerability testing of a sample of deployed CTS machines. Management indicated this was a one-time test in support of the risk assessment needed to complete the CTS Security Plan. Management also indicated it is drafting a memorandum of understanding to be signed by each program office that has CTS equipment. However, although EPA indicated it would take steps to put in place CTS security documents, 3 months have past since our meeting with management and the Security Plan and memorandum of understandings with the EPA offices have not been finalized.

On November 9, 2009, EPA signed an authorization to operate for the CTS equipment. This authorization outlines milestone dates in which the CTS contractor must:

- update the CTS security plan,
- complete an inventory record in the Agency's Registry of EPA Applications and Databases,
- document NIST required security controls for system life cycle management,
- establish Plans of Action and Milestones in the Agency's Automated System Security Evaluation and Remediation Tracking (ASSERT) system to document remediation for high or moderate findings from the independent Risk Assessment,
- establish memoranda of understanding with all appropriate organizations with CTS-defined roles, and
- refine the Contingency Plan.

During our November 9, 2009, meeting with EPA, management indicated that it issued a memorandum to Senior Information Officials regarding their responsibilities for conducting vulnerability testing and that the requirement is in place within the Agency. While management issued a memorandum, this memorandum required the Senior Information Officials to conduct vulnerability testing of the equipment they own. Since the program offices do not own the CTS equipment, management should update its guidance so the Agency Senior Information Officials understand the complete scope of their responsibility for conducting vulnerability testing.

We believe further delays in putting in place a formal security structure for the CTS equipment places EPA's network at great risk. As such, potential security holes may exist and EPA continues to not have an effective management control process to deal with these potential weaknesses.

Recommendations

We recommend the Director, Office of Technology Operations and Planning and Chief Technology Officer, Office of Environmental Information:

1. 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. This procedure should (a) specify the roles and responsibilities for EPA information security personnel and CTS contractors, and (b) require communicating the vulnerability results and resolutions with the applicable EPA program offices.

2. 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. The vulnerability test results should be forwarded to the CTS contractors for remediation.

3. Direct the CTS contractor to remediate identified vulnerabilities in a timely manner and to provide evidence to the initiating Senior Information Official when corrective actions have been taken. This action should continue until management establishes a formal vulnerability testing and management process with CTS.

4. Ensure all key actions outlined in the November 9, 2009, CTS Authorization to Operate are completed by the defined milestone dates.

5. Create Plans of Action and Milestones for the above recommendations in ASSERT.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed To Amount
1	5	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. This procedure should (a) specify the roles and responsibilities for EPA information security personnel and CTS contractors, and (b) require communicating the vulnerability results and resolutions with the applicable EPA program offices.	O	Director, Office of Technology Operations and Planning and Chief Technology Officer, Office of Environmental Information			
2	5	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. The vulnerability test results should be forwarded to the CTS contractors for remediation.	O	Director, Office of Technology Operations and Planning and Chief Technology Officer, Office of Environmental Information			
3	5	Direct the CTS contractor to remediate identified vulnerabilities in a timely manner and to provide evidence to the initiating Senior Information Official when corrective actions have been taken. This action should continue until management establishes a formal vulnerability testing and management process with CTS.	O	Director, Office of Technology Operations and Planning and Chief Technology Officer, Office of Environmental Information			
4	5	Ensure all key actions outlined in the November 9, 2009, CTS Authorization to Operate are completed by the defined milestone dates.	O	Director, Office of Technology Operations and Planning and Chief Technology Officer, Office of Environmental Information			
5	5	Create Plans of Action and Milestones for the above recommendations in ASSERT.	O	Director, Office of Technology Operations and Planning and Chief Technology Officer, Office of Environmental Information			

[1] O = recommendation is open with agreed-to corrective actions pending
C = recommendation is closed with all agreed-to actions completed
U = recommendation is undecided with resolution efforts in progress

Appendix A

Distribution

Office of the Administrator
Acting Assistant Administrator for Environmental Information and Chief Information Officer
Acting Director, Office of Technology Operations and Planning and Chief Technology Officer, Office of Environmental Information
Acting Director, Technology and Information Security Staff, Office of Environmental Information
Agency Follow-up Official (the CFO)
Agency Follow-up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Audit Follow-up Coordinator, Office of Environmental Information
Acting Inspector General