U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

EPA Has Taken Steps to Address Cyber Threats but Key Actions Remain Incomplete

Report No. 11-P-0277

June 23, 2011

Report Contributors:

Patricia H. Hill
Stephen J. Nesbitt
Rudolph M. Brevard
Cheryl Reid
Scott Sammons

Abbreviations

APT	Advanced Persistent Threat
ASSERT	Automated System Security Evaluation and Remediation Tracking
CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Capability
CTS	Customer Technology Solutions
EPA	U.S. Environmental Protection Agency
ETP	Enterprise Transition Plan
FY	Fiscal year
NIST	National Institute of Standards and Technology
OEI	Office of Environmental Information
OIG	Office of Inspector General
US-CERT	United States Computer Emergency Readiness Team

U.S. Environmental Protection Agency
Office of Inspector General

11-P-0277
June 23, 2011

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We reviewed prior audit work to highlight unimplemented actions the U.S. Environmental Protection Agency (EPA) should take to protect network resources from the increase of Advanced Persistent Threats (APTs) within the Agency.

Background

An APT is a cybercrime designed to steal or modify information without detection. These attacks are targeted at organizations, businesses, and political entities, and the perpetrators are usually organized and well funded. APTs are typically tailored, using multiple attack methodologies and tools, for specific targets. After an attack on the specific target has been successful, the threat maintains a foothold on the target for future exploitation.

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

The full report is at:
www.epa.gov/oig/reports/2011/20110623-11-P-0277.pdf

EPA Has Taken Steps to Address Cyber Threats but Key Actions Remain Incomplete

What We Found

News publications have reported that APTs are increasingly prevalent throughout the federal government. In November 2009, the Agency reported 14 compromised systems that were associated with an Office of Inspector General investigation of APTs. By September 2010, the Agency reported that over 7,800 of its systems had communicated with known hostile Internet protocol addresses. These Agency systems potentially could have been compromised by APTs due to these communications. The National Institute of Standards and Technology reports that organizations must enhance risk management and information security governance to guard against APTs.

We issued previous reports and made recommendations that could help the Agency strengthen cyber security practices for combating APTs. However, some of those recommendations remain unimplemented, and we continue to find and report on similar weaknesses at other EPA locations. EPA should address open recommendations, be proactive in implementing agreed-upon actions without further delay, and take steps to improve cyber security practices throughout the entire Agency. If EPA does not take these steps, its information security weaknesses could negatively affect the availability and integrity of all Agency data.

What We Recommend

We recommend that the Assistant Administrator for Environmental Information and Chief Information Officer issue a memorandum to Office of Environmental Information executives stressing the importance of and expectation for completing audit recommendations by the agreed-upon milestone date, strengthen management control processes for monitoring and completing all open and future audit recommendations by the agreed-upon milestone date, and update the Enterprise Transition Plan Information Management segment to define the actions the Agency plans to take to achieve its security target architecture.

The Agency agreed with all the recommendations except for the recommendation to update its audit control process to require the Chief Information Officer to approve milestone dates extensions. Management stated that it implemented a new audit control process giving the Chief Information Officer monthly status reports, and we removed the recommendation.

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

THE INSPECTOR GENERAL

June 23, 2011

MEMORANDUM

SUBJECT: EPA Has Taken Steps to Address Cyber Threats but Key Actions Remain Incomplete
Report No. 11-P-0277

FROM: Arthur A. Elkins, Jr.
Inspector General

TO: Malcolm D. Jackson
Assistant Administrator for Environmental Information and Chief Information Officer

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 direct labor and travel costs for this report are $128,210.

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. Your response will be posted on the OIG's public website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal. We have no objections to the further release of this report to the public. We will post this report to our website at http://www.epa.gov/oig.

If you or your staff have any questions regarding this report, please contact Rudolph M. Brevard, Director, Information Resources Management Assessments, 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

Appendices

Purpose

We sought to highlight unimplemented actions the U.S. Environmental Protection Agency (EPA) should take to protect network resources from the increase of Advanced Persistent Threats (APTs) within the Agency.

Background

An APT is a cybercrime[1] designed to steal or modify information without detection. These attacks are targeted at organizations, businesses, and political entities. The attackers that carry them out are typically organized and well funded. Unlike other virus attacks that may be launched at thousands of random computers on the Internet, APT activities are tailored, using multiple attack methodologies and tools, for specific targets. After a target has been successfully attacked, the attacker maintains a foothold on the target for future exploits. In other words, after an organization fixes the initial vulnerability, the attacker will be able to persist in an automated and hidden mode, remaining on the network unbeknownst to the organization.

In June 2010, the National Institute of Standards and Technology (NIST) reported that federal agencies must take steps in the five areas below to strengthen their risk management and information security governance practices to prepare for these attacks:

1. Develop an organizational risk management and information security strategy.

2. Integrate information security requirements into the organization's core missions and business processes, enterprise architecture, and system development life cycle processes.

3. Allocate management, operational, and technical security controls to organizational information systems and environments of operation based on an enterprise security architecture.

4. Implement a robust continuous monitoring program to understand the ongoing security state of organizational information systems.

5. Develop a strategy and capability for the organization to operate while under attack, conducting critical missions and operations, if necessary, in a degraded or limited mode.

[1] Cybercrime refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

NIST reported that addressing APTs requires a major change in strategic thinking to understand that this class of threat cannot always be kept outside of an agency's defensive perimeters and most likely already resides on its networks. As such, agencies need to employ methods to constrain the threats to ensure the resiliency of their missions and business processes.

Scope and Methodology

We performed this audit from July 2010 through April 2011. We reviewed Office of Inspector General (OIG) audit work and reports issued from fiscal years (FYs) 2008 through 2010, as well as cyber security issues identified during investigations. We reviewed corrective action plans related to open audit recommendations. We reviewed EPA's FY 2010 Agency Financial Report to identify management's actions to address the OIG-identified top management challenge regarding cyber security. We reviewed EPA's Management Audit Tracking System to identify the current milestone dates management identified for completing unimplemented audit recommendations.

Appendix A of this report contains a summary of several OIG audit and evaluation reports and a memorandum assessing EPA's information technology security. We used the analysis of these documents to develop multiple sections of this report.

In December 2010, we provided the Agency a copy of our analysis. We included the Agency's response to our analysis in the report where appropriate. We did not evaluate assertions the Agency made in its response.

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

Increases in APTs Heighten Need to Improve Cyber Security

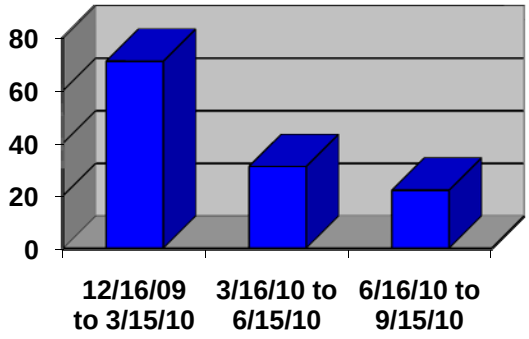
Security articles have reported that APTs are an increasing presence throughout the federal government. In addition, these articles indicated that U.S. government websites, including those of the White House and State Department, have come under broad cyber attacks since July 2009. They believe that a large-scale cyber attack could be as devastating to the U.S. economy and infrastructure as a terrorist bombing.

Four quarterly trend reports covering the period February 2010 through January 2011, issued by the EPA Computer Security Incident Response Capability (CSIRC) center, highlight the need for the Agency to strengthen its ability to respond to cyber threats. According to the reports, there was an average of

565 security incidents per quarter. The two most frequent categories for incidents were (1) unauthorized scans, probes, and attempted access, and (2) investigations into users' reports of cyber attacks. EPA noted that the highest number of incidents pertained to possible malicious code infections, a common attack method used by APTs.

In addition to EPA's efforts to investigate user reports of cyber attacks, EPA has identified a number of computers attempting to communicate with United States Computer Emergency Readiness Team (US-CERT)-identified suspicious domains. From December 2009 to September 2010, EPA reported that it identified over 7,800 potentially compromised computers communicating on the Agency's network.

Figure 1: Average daily number of EPA computers potentially compromised by APTs



Source: OIG analysis.

As shown in figure 1, while EPA experienced a sharp increase in the number of potential compromises during the first 90 days of this period, the Agency noted that the average daily number has decreased over the last 180 days of this period.

EPA's Plans for Combating Current Cyber Threat

In FY 2010, we identified EPA's limited capability to respond to cyber security attacks as a key management challenge confronting the Agency. In EPA's FY 2010 Agency Financial Report, EPA responded that it will continue to manage the threat through Agency-wide vigilance and improved detection capabilities. EPA responded that it had:

- Affirmed a position to support continuous monitoring across the information technology infrastructure
- Made investments to improve capability and increase visibility in its network
- Raised awareness and vigilance across its information security officer community by providing training and placing a security track into its e-Learning portal

EPA noted that it should enhance its information security officer training. Further, EPA stated that it is using existing contracts to augment current contractor staff and pursuing more contract support to focus on detecting APTs.

Audit Work Continues to Highlight Improvements Needed in EPA's Information Security Practices

Our audit work and ongoing analysis continue to highlight how EPA's delays in completing key audit recommendations hinder the Agency's ability to respond to cyber security attacks. Open recommendations for which milestone dates have passed are published semiannually in the OIG's *Compendium of Unimplemented Recommendations*. EPA management extended milestone dates for open recommendations that pertain to cyber security instead of completing corrective actions. This practice has left EPA with sporadically implemented information security practices, which thwart the Agency's ability to promote a focused, multipronged approach in the NIST-recommended areas. Details on EPA with respect to each of the NIST areas follow.

Organizational Information Security Strategy

Given the current threat environment, EPA should increase the effectiveness of its key organizational information security strategies. In particular, we found limited assurance that data in the Automated System Security Evaluation and Remediation Tracking (ASSERT) tool are reliable. In addition, we concluded that the CSIRC center lacks the skills and resources to promptly identify and effectively remedy ongoing cyber threats.

- **ASSERT.** Procedures for oversight and monitoring of self-reported data provide limited assurance that the data in the system are reliable for assessing EPA's computer security program. ASSERT is an online tool to gather information regarding testing and evaluating EPA's information systems. It also tracks progress toward fixing identified security weaknesses. We found that unsupported responses for self-reported information contributed to data quality problems. Limited independent reviews, a lack of training on assessing security controls, and limited internal reporting of these controls also affected data quality. Unreliable data in ASSERT make it difficult for management to know where vulnerabilities exist. Therefore, the system is not reliable for decisionmaking.

- **CSIRC.** Limited followup activities and an overreliance on US-CERT lead us to conclude that the CSIRC center does not have the technical skills or resources needed to promptly identify and remedy ongoing cyber threats. The CSIRC center is EPA's Agency-wide approach to protecting information assets and responding to actual and potential incidents. EPA

has traditionally relied on US-CERT to identify external threats, develop technical solutions, and coordinate government-wide responses to cyber attacks. EPA had not taken steps to modify a contract to provide forensic tools and technical expertise to the CSIRC center until APTs rapidly infiltrated the Agency's network. At the time of this report, EPA had not put in place the new contract. This situation is further compounded by EPA's limited followup activities to investigate the extent to which reported incidents may have threatened and impacted Agency systems. Without these additional skills and resources at the CSIRC center to effectively fight cyber threats, the number of computers and workstations compromised by APTs may continue to rise.

To help ensure the reliability of self-reported data, the Agency stated that it would implement a tool that will provide a platform to build and validate certification and accreditation documentation for all Agency systems. EPA also stated that it is providing the CSIRC center with an array of tools to combat APTs.

Integrated Information Security Requirements

EPA is not integrating information security into all of its business and mission processes. In particular, EPA did not clearly define processes for contractor oversight, follow key system development life cycle requirements, and ensure managerial controls were in place over information security activities.

- **EPA's Contractor Oversight.** EPA has not clearly defined monitoring duties and responsibilities for contractor oversight, and has not trained personnel to perform oversight. Because of the lack of training, personnel are not familiar with their duties and responsibilities regarding oversight of EPA-owned and contractor-operated systems. As such, these systems are at risk that APT activities may occur and go undetected. Undetected APTs can result in loss, destruction, theft, and misuse of sensitive proprietary information. EPA stated it has and will continue to conduct certification and accreditation workshops addressing the Agency's roles and responsibilities related to contractor oversight processes.

- **System Development Life Cycle Processes.** EPA placed contractor equipment into production without a security plan. This plan is a key system development life cycle step and a federal requirement. Security planning assesses risks to EPA's network and is a key factor in management's decision to authorize the equipment for use. As such, management lacked the information it needed to protect the Agency's network from possible threats posed by the over 11,700 contractor computers placed into production.

- **Managerial Controls Over Information Security Activities.** EPA personnel with significant security responsibilities continue to be unable to

show that they executed required information security tasks. In particular, offices lack evidence that testing of information systems security controls takes place as required by federal guidance. Also, the offices lack evidence that contingency plans are tested on an annual basis. Further, EPA lacks a practice to ensure that an authorizing official receives credible information to make risk-based decisions. EPA's business practice for implementing information security processes is to delegate these responsibilities to senior managers throughout the Agency. Stronger management controls are needed to help ensure that security activities are carried out as intended. These stronger controls would help EPA comply with requirements and avoid possible cyber security incidents.

Allocation of Controls Based on Enterprise Security Architecture

EPA has not clearly defined the Information Management segment of its current Enterprise Transition Plan (ETP). The Information Management segment, which addresses information security at an enterprise architecture level, is "Notional," or not in planning. The ETP describes EPA's overarching strategy for modernizing the Agency's infrastructure to achieve its target architecture. The ETP does not clearly define the actions it will take to achieve its security target architecture. Given the rapid rise of APTs on EPA's network, the absence of a clearly defined plan for implementing the Information Management segment shows a lack of commitment on the part of the Agency to address information security from an enterprise-wide perspective. Without this strategy, EPA executives may not be able to make proper investment decisions regarding the necessary tools to combat APTs with an Agency-wide approach.

The Agency stated that all of the new information security tools that it is putting in place are designed to be implemented at an enterprise level.

Continuous Monitoring

EPA has not established an Agency-wide continuous network security monitoring program to identify known vulnerabilities. In this regard, EPA has not completed a key project that would provide its offices with the needed tools to implement an Agency-wide approach for identifying known vulnerabilities. Since 2005, EPA has tried to implement a commercial off-the-shelf network vulnerability tool. Yet, more than 5 years later, EPA is still reviewing the vulnerability management tool. This tool has the ability to identify and correct commonly known security weaknesses. However, project delays have thwarted EPA's ability to move the project beyond the pilot stage. Continuous monitoring is so important that NIST mandated it as a required step for authorizing federal systems to operate.

We conducted 16 vulnerability tests at 14 locations over the past 3 fiscal years. With the exception of one test, the results continued to show that EPA has weaknesses in identifying known critical vulnerabilities. These results occurred

even though US-CERT alert notices for the critical vulnerabilities identified in our latest tests had been issued to the public from up to 6 months to more than 8 years prior to our network test. Therefore, the absence of an Agency-wide continuous monitoring program to identify known vulnerabilities continues to thwart EPA's ability to detect and correct these repeated threats throughout its network.

Also, the absence of an Agency-wide process to identify known vulnerabilities left EPA with over 11,700 unmonitored, contractor-owned computers. Without monitoring, it could be possible for a hacker to gain unauthorized, undetected access to the Agency's network through any of these computers. Lack of an Agency-wide process hinders EPA's ability to protect the integrity and availability of all Agency data. Given that these weaknesses continue to exist, EPA should be more proactive in increasing oversight and monitoring throughout the entire Agency.

EPA stated that it has acquired an Agency-wide vulnerability management tool and is currently deploying it. The Agency also stated that this tool will provide services such as power management, software deployment and inventory management, patch management, network node discovery, vulnerability management, and security configuration management.

Continuity of Operations

EPA has not set up the needed controls to ensure that it complies with NIST guidelines and EPA policies for annual testing of contingency plans for continuity of operations. Current EPA practices do not ensure that failed contingency tests are addressed and all stakeholders are informed of test results in a timely manner. Also, the lack of a contingency plan left EPA, for more than 1 year, without a strategy for recovering the data stored on the over 11,700 contractor-owned computers. Without thorough contingency planning, EPA cannot be sure whether it has a properly designed cyber attack recovery strategy.

EPA stated it would implement a centralized database that will contain contingency and disaster recovery plans for EPA systems.

Recommendations

We recommend that the Assistant Administrator for Environmental Information and Chief Information Officer:

1. Issue a memorandum to Office of Environmental Information executives stressing the importance of and expectation for completing audit recommendations by the agreed-upon milestone date.

2. Strengthen management control processes for monitoring and completing all open and future audit recommendations by the agreed-upon milestone date.

3. Update the ETP Information Management segment to define actions the Agency plans to take to achieve its security target architecture.

Agency Response and OIG Comments

Management stated that over the past 2 years, it made significant personnel and monetary investments and took specific actions to address OIG audits and internal assessments. EPA believes that some of these efforts were not fully accounted for in the draft report. Prior to issuing the draft report, we provided the Agency with the planned report contents and incorporated management's feedback into the draft and final reports. As noted, management agreed with our report except the recommendation to update its internal control practice to require Chief Information Officer (CIO) approval of milestone date extensions. Management stated that it implemented a new process to provide the CIO with monthly status reports on all audits. After this process is fully implemented, we believe it should provide the CIO better oversight of planned corrective actions. Therefore, we updated the report. Management's complete response is in appendix A.

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	7	Issue a memorandum to Office of Environmental Information executives stressing the importance of and expectation for completing audit recommendations by the agreed-upon milestone date.	O	Assistant Administrator for Environmental Information and Chief Information Officer			
2	8	Strengthen management control processes for monitoring and completing all open and future audit recommendations by the agreed-upon milestone date.	O	Assistant Administrator for Environmental Information and Chief Information Officer			
3	8	Update the ETP Information Management segment to define the actions the Agency plans to take to achieve its security target architecture.	O	Assistant Administrator for Environmental Information and Chief Information Officer			

[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

Agency Response to Draft Report

May 11, 2011 (date stamped)

MEMORANDUM

SUBJECT: OEI Response to Draft Report: *EPA Has Taken Steps to Address Cyber Threats But Key Actions Remain Incomplete* (OMS-FY10-0035)

From: Malcolm D. Jackson
Assistant Administrator and Chief Information Officer

To: Patricia H. Hill
Assistant Inspector General for Mission Systems

The purpose of this memorandum is to provide a response to the subject draft report and provide additional clarifications regarding the Office of Environmental Information's (OEI) actions in response to this and prior Office of Inspector General's (OIG) reports regarding the Agency's information security program.

OEI appreciates the OIG's desire to ensure that EPA's information and information systems are secure and available to agency staff. These systems and the information within them are essential to the Agency's success. As the responsible office for information security in EPA, OEI takes very seriously the charge of ensuring proper controls are implemented and functioning properly to minimize risks to personnel, the EPA's mission and the nation's interests.

Over the past two years, OEI has made significant personnel and monetary investments, as well as taken specific actions to address several weaknesses identified in OIG audits and internal assessments. OEI believes that some of these efforts were not fully accounted for in this current draft, which we feel address several of the concerns raised by the OIG in this and prior reports. My staff and I welcome the opportunity to sit with you and your staff to highlight these efforts and to demonstrate how our efforts have in fact addressed many of your concerns and strengthened the Agency's overall information security posture.

Attached you will find OEI's detailed responses to your draft report. While OEI cannot agree with all of the statements in the draft report, we look forward to further discussing these recommendations and draft findings to meet the shared desire of both of our organizations to ensure the most robust information security program possible for EPA.

If you have any questions, please feel free to contact me or Robert McKinney, EPA's Senior Agency Information Security Officer.

cc:
Renee Wynn, Acting Principal Deputy Assistant Administrator, OEI
Vaughn Noga, Director, Office of Technology Operations and Planning
Robert F. McKinney Jr., Senior Agency Information Security Officer

ATTACHMENT: OEI's Detailed Response to Draft Report: *EPA Has Taken Steps to Address Cyber Threats buy Key Actions Remain Incomplete* (OMS-FY10-0035)

The following are OEI's responses to the four recommendations identified in the draft report:

1. Issue a memorandum to Office of Environmental Information executives stressing the importance of and expectation for completing audit recommendations by the agreed-upon milestone date.

OEI agrees with this recommendation and the AA/CIO will issue a memorandum. Just for clarification however, the AA/CIO has already made the audit program a priority on an ongoing basis that stresses the importance of addressing findings effectively and expeditiously. The OEI Audit Coordinator provides the OEI AA and PDAA monthly status reports of all audits and OEI executives must provide updates to the OEI AA in Quarterly Business Reviews. OEI believes that the memorandum, new business processes and this personal attention placed on the issue by the AA/CIO should fully address this recommendation.

2. Strengthen management control processes for monitoring and completing all open and future audit recommendations by the agreed-upon milestone date.

OEI agrees with recommendation 2 and as stated above believes we have taken proactive steps to strengthen the management control processes. OEI believes recommendation 2 has been addressed.

3. Update the process to require the Chief Information Officer's documented approval to extend agreed-upon milestone dates.

OEI respectfully disagrees with this recommendation, not in substance but as a matter of policy. The controlling policy authority for audit follow up is found in EPA Manual 2750 CH2, *EPA's AUDIT MANAGEMENT PROCESS*, dated 12/1998. Unless the AA/CIO is the action official, OEI is unable to find a requirement that the AA be required to provide documented approval to make modifications to milestones. OEI's position is that we, like any other AAship in the Agency, should follow the OIG's established procedures outlined in the Manual.

4. Update the Enterprise Transition Plan (ETP) Information Management segment to define actions the Agency plans to take to achieve its security target architecture.

OEI agrees with recommendation 4. The Agency's ETP was renamed EPA Modernization Blueprint in February 2011 and describes the overarching strategy for modernizing the Agency's infrastructure and transition process in support of the business, as well as the specific IT projects and approach EPA will use to achieve its target architecture. As such, OEI plans to update the EPA Modernization Blueprint in February 2012 with specifics regarding the roadmap and the acquisition strategy that provides enhanced security capabilities for the Agency.
OEI stands committed to working with your staff on completing the remaining open recommendations found in Appendix B of this Draft Report.

Appendix B

Summaries of OIG Information Security Reports and Memorandum

The OIG has published several audit and evaluation reports and a memorandum assessing EPA's information technology security. Selections of these are summarized below. The complete reports and memorandum can be accessed at http://www.epa.gov/oig/rpts_docs.htm.

OIG Technical Vulnerability Assessment Reports (FYs 2008–2010)

The OIG conducted testing at various locations to identify network vulnerabilities. If not resolved, vulnerabilities can expose EPA's assets to unauthorized access and potentially harm the Agency's networks.

The testing, done as part of the Federal Information Security Management Act review, disclosed several high-risk and medium-risk vulnerabilities at the following EPA locations (the report publication number and date are in parentheses):

- Andrew W. Breidenbach Environmental Research Center, Cincinnati, Ohio *(10-P-0210, September 7, 2010)*
- Erlanger Building, Erlanger, Kentucky *(10-P-0211, September 7, 2010)*
- Ronald Reagan Building, Washington, DC *(10-P-0212, September 7, 2010)*
- Region 4, Atlanta, Georgia *(10-P-0213, September 7, 2010)*
- Research Triangle Park Finance Center, Research Triangle Park, North Carolina *(09-P-0227, August 31, 2009)*
- Great Lakes National Program Office, Chicago, Illinois *(09-P-0185, June 30, 2009)*
- National Computer Center, Research Triangle Park, North Carolina *(09-P-0186, June 30, 2009)*
- Region 8, Denver, Colorado *(09-P-0187, June 30, 2009)*
- Potomac Yard Buildings, Arlington, Virginia *(09-P-0188, June 30, 2009)*
- 1310 L Street Building, Washington, DC *(09-P-0189, June 30, 2009)*
- EPA Headquarters, Washington, DC *(09-P-0097, February 23, 2009)*
- Research Triangle Park Campus, Research Triangle Park, North Carolina *(09-P-0055, December 9, 2008)*
- Las Vegas Finance Center, Las Vegas, Nevada *(09-P-0054, December 9, 2008)*
- Radiation and Indoor Environments National Laboratory, Las Vegas, Nevada *(09-P-0053, December 9, 2008)*
- Region 9, San Francisco, California *(09-P-0052, December 9, 2008)*

Improvements Needed in Key EPA Information System Security Practices (10 P-0146, June 15, 2010)

Williams, Adley & Company, LLP (Williams Adley), a firm that the OIG contracted with to perform the review, found that EPA program offices lacked evidence that they planned and executed tests of information system security controls as required by federal requirements. In addition, Williams Adley found that contingency plans developed and maintained by program offices were not current and accurate, and the certification and accreditation process and review of security plans needed improvements. EPA also had two authoritative system inventories that did not reconcile. Finally, EPA had contractor-owned and -operated systems in operation without proper oversight monitoring.

Williams Adley's recommendations to the Director of the Office of Technology Operations and Planning included communicating and training EPA's information security community on testing and documenting information systems security controls. Williams Adley also recommended that the Director enhance the quality assurance process to verify that self-assessments evaluate all required security controls.

Memorandum on EPA's Fiscal Year 2010 Management Challenges (May 11, 2010)

EPA has a limited capacity to effectively respond to external network threats despite reports from security experts that APTs designed to steal or modify information without detection are becoming more prevalent throughout the government. Our ongoing analysis shows that the Agency has not addressed the challenge of remediating escalating threats from cyber security attacks. To date, EPA has reported that over 5,000 servers and user workstations may have been compromised as a result of recent cyber security attacks.[2] These compromised systems extend to every EPA regional office and headquarters. Moreover, ongoing work disclosed that EPA could not identify the owners of approximately 10 percent of the Internet Protocol addresses that are potentially compromised due to an APT.

EPA leadership must meet this challenge head-on by sufficiently funding the development of a real capability to identify and investigate attacks against EPA's computer and network systems. Moreover, Congress should fully consider EPA's new budget proposals to ensure that the Agency has the fiscal capacity to tackle this challenge. EPA management cannot continue to rely on a "pay as you go" mentality; rather, EPA needs an established budget for managing information technology infrastructure and security. Key leaders must understand the threats that exist to EPA's confidential business information and the importance of minimizing those risks. Furthermore, the Chief Information Officer and Office of Technology Operations and Planning leadership should carefully study and trust the classified intelligence materials provided to them regarding threats against government domains. The Agency should also develop a method to

[2] As of September 15, 2010, the number of servers and user workstations that may have been compromised had increased to over 7,800.

disseminate sensitive information, including classified data, to senior leadership and technical staff, especially when the network is reportedly (5,000 plus systems) compromised.

Self-Reported Data Unreliable for Assessing EPA's Computer Security Program **(10 P-0058, February 2, 2010)**

The oversight and monitoring procedures for ASSERT provide limited assurance the data are reliable for assessing EPA's computer security program. As a result:

- Unsubstantiated responses for self-reported information contribute to data quality problems.
- Limited independent reviews and lack of followup inhibit EPA's ability to identify and correct data inaccuracies.
- Independent reviews lack coordination with certification and accreditation activities.
- Information security personnel believe they need more training on how to assess security controls and feel pressure to answer system security questions in a positive manner.
- Limited internal reporting on required security controls and missing information in security plans inhibit external reporting.

Further, incomplete security documentation raises concerns as to whether the ASSERT application contractor is meeting federal requirements.

Improved Security Planning Needed for the Customer Technology Solutions Project **(10 P-0028, November 16, 2009)**

EPA lacks a process to routinely test Customer Technology Solutions (CTS) equipment for known vulnerabilities and to correct identified threats. Further, 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 NIST. 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.

***Project Delays Prevent EPA from Implementing an Agency-wide Information Security Vulnerability Management Program* (09-P-0240, September 21, 2009)**

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 Office of Management and Budget Circular A-123. EPA is updating its audit management and oversight policies; we provided suggestions for strengthening them.

Appendix C

Open Recommendations

Below is a list of open audit recommendations, the implementation of which by the Office of Environmental Information would improve information security controls in Agency systems, programs, processes, or procedures. These recommendations, when implemented, could help the Agency strengthen cyber security areas and respond to APTs. Moreover, it appears the Agency should evaluate implementing these recommendations across the Agency (not just in locations listed below).

OIG open audit recommendations as of May 24, 2011

Security Configuration and Monitoring of EPA's Remote Access Methods Need Improvement, Report No. 2005-P-00011		
Open recommendation	**Planned completion date**	**Revised completion date**
Develop and implement a security-monitoring program that includes testing all servers, and require all system administrators to register their servers with the National Technology Services Division and participate in the security-monitoring program.	9/30/2005	6/30/2011
Expand the Agency's security-monitoring program to include using a variety of network vulnerability scanning tools to monitor registered servers.	9/30/2005	6/30/2011
Establish and implement a process to ensure program and regional offices conduct regular security monitoring that includes vulnerability scanning.	9/30/2005	6/30/2011
***EPA Could Improve Processes for Managing Contracting Systems and Reporting Incidents*, Report No. 2007-P-00007**		
Open recommendation	**Planned completion date**	**Revised completion date**
Develop and implement guidance that EPA offices can use to identify appropriate contractor systems that contain EPA data.	9/18/2008	9/15/2011
***EPA Could Improve Controls Over Mainframe System Software*, Report No. 2007-P-00008**		
Open recommendation	**Planned completion date**	**Revised completion date**
Complete efforts to update the *Office of Environmental Information (OEI) Information Security Manual* and the *EPA Information Security Manual*. Subsequent to finalizing the changes, ensure the manuals are (1) reviewed timely by EPA management for adequacy, accuracy, and completeness; and (2) approved by EPA management in a timely manner.	9/18/2008	3/30/2013

***Results of Technical Network Vulnerability Assessment: EPA Headquarters*, Report No. 09-P-0097**		
Open recommendation	**Planned completion date**	**Revised completion date**
Develop and implement procedures to periodically review the data within IP Registry for accuracy and completeness. These procedures should include, but not be limited to, documenting any findings, issuing correspondences to the responsible Program Offices to resolve the findings and maintaining documents of all resolutions.	12/31/2010	4/30/2011
***Project Delays Prevent EPA from Implementing an Agency-wide Information Security Vulnerability Management Program*, Report No. 09-P-0240**		
Open recommendation	**Planned completion date**	**Revised completion date**
Issue an updated memorandum that: (a) reflects the current version of NIST Special Publication 800-53; (b) requires continuous scanning/remediation on at least a monthly basis; (c) requires continuous scanning/remediation be performed using two tools concurrently; and (d) specifies what tools and resources OEI can actually provide to help the applicable personnel fulfill these responsibilities and what the applicable organization will have to obtain on their own to perform these responsibilities.	4/01/2011	8/30/2011

Source: EPA OIG.

Appendix D

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information and Chief Information Officer
Agency Followup Official (the CFO)
Agency Followup Coordinator
Director, Office of Technology Operations and Planning, Office of Environmental Information
General Counsel
Associate Administrator for Congressional and Intergovernmental Affairs
Associate Administrator for External Affairs and Environmental Education
Audit Followup Coordinator, Office of Environmental Information