U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Improvements Needed in EPA’s Network Security Monitoring Program

Report No. 12-P-0899 **September 27, 2012**

Scan this mobile
code to learn more
about the EPA OIG.

Report Contributors:

Rudolph M. Brevard
Cheryl Reid
Vincent Campbell
Neven Soliman
Kyle Denning

Abbreviations

ASSERT	Automated System Security Evaluation and Remediation Tracking
CERT	Computer Emergency Response Team
CSIRC	Computer Security Incident Response Capability Center
CTS	Customer Technology Solutions
EPA	U.S. Environmental Protection Agency
ISO	Information Security Officer
IT	Information Technology
NCC	National Computer Center
NIST	National Institute of Standards and Technology
OEI	Office of Environmental Information
OIG	Office of Inspector General
OTOP	Office of Technology Operations and Planning
POA&M	Plans of Actions and Milestones
SIEM	Security Incident and Event Management
SP	Special Publication
TISS	Technology and Information Security Staff

Hotline

To report fraud, waste, or abuse, contact us through one of the following methods:

e-mail: OIG_Hotline@epa.gov
phone: 1-888-546-8740
fax: 202-566-2599
online: http://www.epa.gov/oig/hotline.htm

write: EPA Inspector General Hotline
1200 Pennsylvania Avenue NW
Mailcode 2431T
Washington, DC 20460

U.S. Environmental Protection Agency
Office of Inspector General

12-P-0899
September 27, 2012

At a Glance

Why We Did This Review

The U.S. Environmental Protection Agency (EPA) Office of Inspector General (OIG) conducted this audit to (1) identify which tools EPA uses to identify, analyze, and resolve cyber-security incidents; (2) identify steps implemented to resolve known weaknesses in its incidence response capabilities; and (3) evaluate how users report security incidents.

Continually monitoring network threats through intrusion detection and prevention systems and other mechanisms is essential. Establishing clear procedures for assessing the current and potential business impact of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data.

This report addresses the following EPA Goal or Cross-Cutting Strategy:

- *Strengthening EPA's Workforce and Capabilities*

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

The full report is at:
www.epa.gov/oig/reports/2012/20120927-12-P-0899.pdf

Improvements Needed in EPA's Network Security Monitoring Program

What We Found

EPA's deployment of a Security Incident and Event Management (SIEM) tool did not comply with EPA's system life cycle management procedures, which require planning project activities to include resources needed, schedules, and structured training sessions. EPA did not develop a comprehensive deployment strategy for the SIEM tool to incorporate all of EPA's offices or a formal training program on how to use the tool. When EPA staff are not able to use an information technology investment, the investment has limited value in meeting organizational goals and users' needs.

EPA does not have a computer security log management policy consistent with federal requirements. While EPA has a policy governing minimum system auditing activities to be logged, EPA has yet to define a policy for audit log storage and disposal requirements along with log management roles and responsibilities. EPA risks not having logged data available when needed, and program officials may not implement needed security controls.

EPA did not follow up with staff to confirm whether corrective actions were taken to address known information security weaknesses. EPA had not taken steps to address weaknesses identified from internal reviews as required. Known vulnerabilities that remain unremediated could leave EPA's information and assets exposed to unauthorized access.

Recommendations and Planned Agency Corrective Actions

We recommended that the Assistant Administrator for Environmental Information develop and implement a strategy to incorporate EPA's headquarters program offices within the SIEM environment, develop and implement a formal training program for the SIEM tool, develop a policy or revise the Agency's Information Security Policy to comply with audit logging requirements, and require that the Senior Agency Information Security Officer be addressed on all Office of Environmental Information security reports and reviews.

Office of Environmental Information officials concurred with and agreed to take corrective actions to address all recommendations.

Noteworthy Achievements

We found that EPA employees are aware of the reporting procedures for when they experience an information security incident. Additionally, EPA has recently deployed technical tools to combat cyber-security attacks and conduct forensic analyses of security activity.

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

THE INSPECTOR GENERAL

September 27, 2012

MEMORANDUM

SUBJECT: Improvements Needed in EPA's Network Security Monitoring Program
Report No. 12-P-0899

FROM: Arthur A. Elkins, Jr. Arthur A. Elkins

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.

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 action plan for agreed-upon actions, including milestone dates. Recommendations marked unresolved due to a "TBD" planned completion date require a milestone date. 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 has any questions regarding this report, please contact Patricia Hill, Assistant Inspector General, Office of Mission Systems, at (202) 566-0894 or hill.patricia@epa.gov; or Rudolph M. Brevard, Director, Information Resources Management Assessments, at (202) 566-0893 or brevard.rudy@epa.gov.

Table of Contents

Chapters

Appendices

Chapter 1
Introduction

Purpose

We sought to determine:

- What tools has the U.S. Environmental Protection Agency (EPA) implemented to increase its capability to promptly identify, analyze, and resolve cyber-security incidents against the Agency's network?
- What steps has EPA implemented to resolve known weaknesses in its incident response capability?
- Could EPA make improvements in how users report security incidents?

Background

A computer security incident is a violation or threat of a violation of computer security policies or standard security practices. Computer security-related threats have not only increased and become more diverse, but can cause more damage. Preventive actions based on risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is needed for the quick detection of incidents and to minimize loss and destruction of data, mitigate the weaknesses that were exploited, and restore computing services. Continual monitoring of threats through intrusion detection and prevention systems and other mechanisms is essential. Establishing clear procedures to assess current and potential business impacts of incidents is critical, as is putting in place effective methods to collect, analyze, and report data.

The Assistant Administrator for Environmental Information, who is also EPA's Chief Information Officer, is charged under the Federal Information Security Management Act with providing leadership to ensure the security of EPA's information technology (IT) resources. The Assistant Administrator for Environmental Information designates a Senior Agency Information Security Officer, who is responsible for managing Agency compliance with federal information security requirements.

EPA's Office of Technology Operations and Planning (OTOP), within the Office of Environmental Information (OEI), is responsible for the policy, management, and implementation of EPA's IT infrastructure. Within OTOP, Technology and Information Security Staff (TISS) are responsible for managing the operation of EPA's IT security program. TISS is responsible for deploying and managing EPA's Security Incident and Event Management (SIEM) tool. SIEM documents show that EPA's information security staff can use the SIEM tool to (1) comply with federally required log review and correlation activities, and (2) reduce the level of effort on administrative staff. TISS acquired a SIEM tool in May 2010. TISS documentation indicates that the SIEM tool would be used to perform real-time analysis of security alerts to help respond to security attacks faster and create log security data and compliance reports.

During years 2010-2011, EPA invested over $4.1 million in several automated tools to strengthen the security of the Agency's network infrastructure. OEI, Region 7, and Region 8 information security personnel manage the tools we reviewed. See Appendix A for additional details on these tools.

EPA uses the Automated System Security Evaluation and Remediation Tracking (ASSERT) system to prepare Federal Information Security Management Act reports. ASSERT provides systems owners and managers with an understanding of the system's risks, security controls needed to address risks, and a plan of actions and milestones to remediate risks.

Noteworthy Achievements

We found that EPA employees are aware of reporting procedures for when they experience an information security incident. OTOP deployed forensic and SIEM tools to strengthen EPA network monitoring. OTOP staff indicated that the forensic tool could be used to identify rogue executable files on EPA workstations. TISS documentation indicated that the SIEM tool performs real-time analysis of security alerts, and is available for EPA's information security staff to perform audit logging.

Scope and Methodology

Our audit work commenced March 2011 and was completed in June 2012. We conducted our audit work at EPA headquarters in Washington, DC; National Computer Center, Research Triangle Park, North Carolina; Region 7 headquarters in Kansas City, Kansas; and Region 8 headquarters in Denver, Colorado. 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, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We reviewed federal regulations and EPA policies and procedures. We collected and reviewed purchase orders and contract agreements, but did not conduct any tests to determine whether contractors complied with contract terms and conditions. We interviewed EPA headquarters and regional information security staff on technical tools used to monitor and analyze network traffic. We obtained an understanding of each tool's use, purpose, cost, and function. We did random interviews of headquarters and regional staff to assess their knowledge for reporting incidents.

We conducted follow-up on two prior EPA Office of Inspector General (OIG) security audits on EPA's network security monitoring program.

- In EPA OIG Report No. 2005-P-00011 *Security Configuration and Monitoring of EPA's Remote Access Methods Need Improvement*, dated March 22, 2005, we recommended that OTOP develop and implement a security-monitoring program that includes testing all servers.

- In 2009, we followed up on the above report in EPA OIG Report No. 09-P-0240, *Project Delays Prevent EPA from Implementing an Agency-wide Information Security Vulnerability Management Program,* dated September 21, 2009. We had sought to determine whether the Agency had implemented an Agency-wide network security monitoring program. We concluded that EPA still had not established an Agency-wide network security monitoring program because EPA did not take alternative action when the monitoring project experienced significant delays. Additionally, EPA offices did not regularly evaluate the effectiveness of actions taken to correct identified deficiencies as required by the Office of Management and Budget.

Chapter 2
Security Incident and Event Management Tool Deployment Lacks Key Activities

EPA’s deployment of a SIEM tool did not comply with Agency requirements for deploying IT investments. EPA's system life cycle management procedures require planning project activities to include resources needed, schedules, and structured training sessions. In particular, EPA had not taken steps to ensure the successful implementation of the SIEM tool by putting in place processes to manage the turnover of key personnel critical to the project's success, making sure plans included all EPA offices, ensuring all responsible individuals have access to management reports generated by the tool, maintaining communications with EPA offices to ensure they were informed of the tool's deployment schedule, and providing training so that offices could use the tool once it was implemented in their respective offices. Without having such plans in place, EPA risks that the SIEM tool would not provide effective network monitoring. When EPA staff are not able to use an IT investment, that investment has limited value in meeting organizational goals and users’ needs.

Headquarters Offices Need a SIEM Tool Implementation Strategy

TISS lacks a fully developed strategy to include EPA’s headquarters program offices within the SIEM’s environment. TISS’s documents showed a strategy that included each of EPA’s regional offices within the SIEM’s environment. However, efforts to include headquarters program offices fell short due to turnover of technical staff and TISS having discontinued meetings with program office staff on using the SIEM tool. As such, ten program offices do not have their headquarters servers logged by the SIEM tool.

Although regional information security officers (ISOs) have access to review daily log activity and receive daily log reports, ten headquarters ISOs do not have access to the SIEM tool or receive the daily reports. Each program office manages numerous assets connected to EPA’s network, with some assets containing sensitive information such as personally identifiable information. We interviewed several headquarters ISOs who expressed interest in using the SIEM tool, but they said barriers have hindered the use of the SIEM tool in their office. Specifically, they cited a lack of (a) access to the tool, (b) demonstration of the tool’s capabilities, and (c) follow-up communication from TISS.

TISS management stated that bringing devices within the SIEM architecture is based on a first-come, first-serve basis. TISS had not developed a strategy that included a priority list based on EPA’s mission-critical and business processes.

Such an approach would have provided TISS a systematic approach for including each program within the SIEM's architecture based on the level of risk.

With a majority of EPA's program offices not using the SIEM tool to monitor security of their assets, the assessment of the security controls associated with log reviews and event correlations may not be as efficient and effective compared to those EPA offices using the SIEM's robust technology. Also, headquarters program offices do not have access to an automated tool that could provide an extra level of analysis to help with recognizing patterns and relationships within data that may escape manual analyses.

TISS provided an updated project plan in February 2012. However, milestone dates have not been finalized as to when headquarters program offices will be incorporated within the SIEM architecture.

Training on SIEM Tool's Utilities Needs Improvements

TISS did not develop a structured training plan to use with the SIEM tool. EPA's system life cycle management procedures require the development of a training plan and user manual when training users of new IT investments. The training plan should outline objectives, target audience, strategies, and curriculum.

TISS conducted informal training sessions with EPA's regional ISOs to address questions on tool usage and how to generate reports. Those sessions did not include written agendas or discussion topics. Regional ISOs said that the training sessions needed more emphasis on how the SIEM tool could be used to perform detailed security analyses. Further, headquarters ISOs were not aware of the training sessions. TISS said the training sessions were stopped due to staff changes.

TISS also sends daily SIEM reports to EPA's ISOs for review and analysis. However, EPA's ISOs stated the files were too large to perform detailed analyses and were limited to spreadsheet queries. Some ISOs said they want to be able to filter the log data by event type. The ISOs can create custom reports if they know programming language. TISS had not created a user guide on how to generate security reports, which the ISOs stated would be of immense value in obtaining hands-on experience with the SIEM tool.

Without a structured training curriculum, users' needs are not being met and the continued use of the SIEM tool by EPA's information security staff will be of limited value in performing information security activities.

Recommendations

We recommend that the Assistant Administrator for Environmental Information:

1. Develop and implement a strategy with milestone dates to incorporate EPA's headquarters program offices within the SIEM environment.

2. Develop and implement a formal training program that will meet EPA's information security staff needs in using the SIEM tool. The training program should include a user guide on using the SIEM tool to generate reports and developing customized reports for filtering known and suspicious events.

Agency Comments and OIG Evaluation

OEI officials concurred with and agreed to take corrective actions to address all recommendations. We believe these corrective actions, when implemented, will address the intent of our recommendations.

Appendix C contains the Agency's complete response to the report.

Chapter 3
Improvements Needed in EPA's Computer Security Log Management Practices

EPA does not have a computer security log management policy that complies with federal requirements. While EPA has a policy governing minimum system auditing activities to be logged, EPA has yet to define a policy for audit log storage and disposal requirements. EPA recently implemented its SIEM tool. However, the Agency has yet to finalize its guidance to govern the roles and responsibilities for the log management infrastructure. The National Institute of Standards and Technology (NIST) requires agencies to define mandatory requirements for these activities. Without activity definitions, EPA risks logged data not being available when needed for event analysis. Furthermore, without clearly defined roles and responsibilities for the log management infrastructure, EPA risks having program office officials responsible for securing their systems not implement needed security controls for log management.

EPA Policy Lacks Some Log Management Requirements

Three sites visited had audit logging procedures, but none of the sites had consistent procedures. For example, one site's procedures did not include requirements for proper log storage and disposal, while the other sites had inconsistent storage and disposal procedures. NIST Special Publication (SP) 800-92, "Guide to Computer Security Log Management," dated September 2006, states that an organization should develop policies that clearly define mandatory requirements for log management activities including log generation, log storage and disposal, and log analysis.

EPA offices defined and implemented their own respective logging procedures because the Agency's policy does not define mandatory audit logging requirements. EPA issued an Interim Agency Information Security Policy in April 2012 to supersede its Agency Network Security Policy, however this policy still does not address key log management elements such as proper log storage and disposal. The lack of a clearly defined audit logging policy could lead additional EPA offices to create inconsistent logging practices across the Agency, and may jeopardize the availability of EPA's logging information when needed for investigating suspicious activity that may not be monitored by the SIEM tool.

Log Management Infrastructure Lacks Approved Roles and Responsibilities

While EPA defined the roles and responsibilities for the SIEM infrastructure within the draft “Enterprise Reference Guide” dated June 2011, the Agency has yet to finalize these requirements. NIST SP 800-92 states that as part of the log management planning process, an organization should define the roles and responsibilities of individuals and teams expected to be involved in log management.

We found that EPA had not developed a policy to define the roles and responsibilities for log management. We believe that the lack of a policy to reinforce how EPA would use the SIEM infrastructure to comply with the log review requirements of NIST SP 800-53, “Recommended Security Controls for Federal Information Systems,” contributed to the issues identified in chapter 2 of this report. Furthermore, EPA intended the SIEM tool to be used to provide information beyond what is required to meet basic NIST SP 800-53 log review requirements. Without a clearly defined policy outlining respective roles within the log management infrastructure, the SIEM tool may not meet its intended purpose.

Recommendations

We recommend that the Assistant Administrator for Environmental Information:

3. Develop a policy or revise the Agency’s Information Security Policy to comply with NIST SP 800-92. This policy should include, but not be limited to, defining log storage and disposal requirements and roles and responsibilities for the log management infrastructure.

4. Finalize the SIEM tool’s “Enterprise Reference Guide.”

Agency Comments and OIG Evaluation

OEI officials concurred with and agreed to take corrective actions to address all recommendations. We believe these corrective actions, when implemented, will address the intent of our recommendations. OEI officials also listed “TBD” (to be determined) for the planned completion date for recommendation 3. We list the status of this recommendation as unresolved. In our transmittal memorandum, we request OEI officials to provide milestone dates in the 90-day response.

Appendix C contains the Agency’s complete response to the report.

Chapter 4
EPA Lacks an Oversight Process to Remediate Information Security Weaknesses

EPA did not follow up with staff to confirm that corrective actions were taken to address known information security weaknesses. EPA had not addressed weaknesses identified by internal reviews. Office of Management and Budget Circular A-123, "Management Accountability and Control," states managers are responsible for taking timely and effective actions to correct identified deficiencies. OEI, which is responsible for securing EPA's network from internal and external exploits, has not developed a process to verify that known weaknesses have been addressed. As a result, known vulnerabilities remained unremediated and key steps to resolve those weaknesses remain unaddressed, which could leave EPA information exposed to unauthorized access.

EPA Did Not Address Recommendations From Internal Reviews

From 2009 to 2010, three internal reviews were conducted on EPA's information security program. EPA prepared an internal document titled "Clampi Infection Lessons Learned Document" that summarized EPA's response to a Trojan horse infection. A Trojan horse is a computer program that is hiding a virus or other potentially damaging program. A Trojan horse can be a program that purports to do one action when, in fact, it is performing a malicious action on a computer. Trojan horses can be included in software that is downloaded for free or as attachments in email messages. EPA contracted with the Computer Emergency Response Team (CERT) Program at the Carnegie Mellon University's Software Engineering Institute and with Booz Allen Hamilton to conduct separate reviews of EPA's information security program. We found proper points of contacts were difficult to obtain and plans of actions and milestones (POA&Ms) were either not created or were not created until our audit was underway. EPA's POA&Ms procedures state that any IT security finding and recommendation from reviews, audits, assessments, tests, or other sources (including but not limited to incidents), must be analyzed and categorized as to the level of risk (high, medium, low) and a determination made for appropriate action to be taken for the weaknesses identified. Table 1 identifies the names of the reports and the number of recommendations reviewed, not addressed, and without POA&Ms.

Table 1: Three internal reports reviewed with status of recommendations

Title of Agency internal review	No. of report recommendations	No. of recommendations not addressed	No. of recommendations without POA&Ms
Clampi Infection Lessons Learned	53	6	7
Carnegie Mellon	31	17	31
Booz Allen Hamilton	19	0	19
Totals	**103**	**23**	**57**

Source: Clampi Infection Lessons Learned document, Carnegie Mellon report, and Booz Allen Hamilton report. OIG-generated.

The **Clampi Infection Lessons Learned** document resulted from a Trojan horse infection that occurred within EPA in July 2009. Based on meetings with EPA, we found that there was no central point of contact responsible to ensure EPA staff addressed each recommendation. In some cases, EPA staff could not provide any evidence on how the issues and recommendations were addressed. We also found that some recommendations were not addressed and, in some cases, POA&Ms were created after we started fieldwork, or 2 years after the Clampi Infection occurred.

The **Carnegie Mellon** report, issued in August 2009, appraised six areas within EPA's information security program using the CERT Resiliency Engineering Framework. We found that EPA's management had neither taken corrective actions nor created POA&Ms to address the findings. As a result of our findings, TISS developed a strategic plan covering fiscal years 2011 through 2016 to manage the report's findings. We found that the strategic plan addressed sections of the report except for issues on global strengths and weaknesses. We also found that POA&Ms were not created for other areas reviewed.

The **Booz Allen Hamilton** document, issued in August 2010, identified procedural and operational deficiencies with EPA's incident handling capabilities when dealing with Advanced Persistent Threats. These threats are adversaries who can bypass virtually all of today's best practices and have the ability to establish and maintain a long-term presence on target networks. When we followed up on the issues, TISS developed a strategic plan to address the report's findings. Although the strategic plan did not include an authoritative corrective action plan, we considered the strategic plan a managerial approach to remediate known weaknesses. TISS had not created POA&Ms in EPA's ASSERT system to manage the document's findings and to ensure accountability is assigned.

Appendix B identifies the documents' findings and recommendations that remain unaddressed.

National Computer Center Does Not Follow Up on Internally Conducted Network Scans

OEI does not require system owners to provide a response on how they addressed vulnerabilities identified during monthly network testing**.** Further, OEI does not follow up with system owners to confirm that identified vulnerabilities have been addressed. Office of Management and Budget's Circular A-123 requires managers to take timely and effective action to correct deficiencies identified by a variety of sources. The circular also states that correcting deficiencies is an integral part of management accountability and must be considered a priority by the Agency. National Computer Center (NCC) staff stated that it was not their responsibility to ensure that the vulnerabilities are addressed. Therefore, there is no assurance that identified vulnerabilities are being addressed or monitored, which could expose EPA's network to security attacks.

In EPA OIG Report No. 2005-P-00011, *Security Configuration and Monitoring of EPA's Remote Access Methods Need Improvement*, dated March 22, 2005, we recommended that OTOP develop and implement a security-monitoring program that includes testing all servers. Further, in EPA OIG Report No. 09-P-0240, *Project Delays Prevent EPA from Implementing an Agency-wide Information Security Vulnerability Management Program*, dated September 21, 2009, we concluded that EPA still had not established an Agency-wide network security monitoring program because EPA did not take alternative action when the monitoring project experienced significant delays.

We looked at the NCC Foundstone tool during the conduct of this audit and found that OEI's NCC staff conduct monthly vulnerability scans of EPA's network and forward scan results to the appropriate contacts for action. However, NCC staff do not follow up nor require system owners to respond so that NCC can confirm that scan results have been addressed. NCC staff stated they provide the tools and the support but regional and program office staff are responsible for taking action. NCC staff does not rescan those servers at a later date to confirm vulnerabilities were remediated. We made our initial recommendation in 2005 but an EPA-wide vulnerability management and remediation process is still not in place. Therefore, there is no assurance that EPA's information security staff is remediating vulnerabilities in a timely manner, and such vulnerabilities could expose EPA's assets to unauthorized access and potential harm to the network.

Recommendations

We recommend that the Assistant Administrator for Environmental Information:

5. Issue a memorandum to OEI officials requiring the Senior Agency Information Security Officer be the addressee on all internal security reports and reviews in order to ensure identified weaknesses are recorded within the Agency's security weakness tracking system.

6. Create POA&Ms for all recommendations applicable to Agency internal reports identified in Appendix B.

7. Develop and implement a process to verify that identified weaknesses in Appendix B are addressed and decisions are documented on actions taken.

8. Develop and implement a process to verify that regions and program office staff address vulnerabilities from NCC scans.

Agency Comments and OIG Evaluation

OEI officials concurred with recommendations 6 through 8. Recommendation 5 originally required a written appointment of a central point of contact for tracking the completion of weaknesses discovered during internal assessments. In its response, OEI stated that the Agency's Senior Agency Information Security Officer is appointed as the central Agency contact for tracking remediation action. However, our audit work disclosed that the points of contact were difficult to obtain and POA&Ms were not created. We modified our recommendation to state that the Assistant Administrator for Environmental Information and Chief Information Officer should direct his staff to provide reports on all security reports and reviews to the Senior Agency Information Security Officer. The Agency agreed to the modified recommendation. OEI officials concurred with and agreed to take corrective actions to address all recommendations. We believe these corrective actions, when implemented, will address the intent of our recommendations. OEI officials also listed "TBD" (to be determined) for planned completion dates for recommendations 5, 6, and 7. We list the status of these recommendations as unresolved. In our transmittal memorandum, we request OEI officials to provide milestone dates in the 90-day response.

Appendix C contains the Agency's complete response to the report.

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	6	Develop and implement a strategy with milestone dates to incorporate EPA's headquarters program offices within the SIEM environment.	O	Assistant Administrator for Environmental Information	12/31/13		
2	6	Develop and implement a formal training program that will meet EPA's information security staff needs in using the SIEM tool. The training program should include a user guide on using the SIEM tool to generate reports and developing customized reports for filtering known and suspicious events.	O	Assistant Administrator for Environmental Information	12/31/12		
3	8	Develop a policy or revise the Agency's Information Security Policy to comply with NIST SP 800-92. This policy should include, but not be limited to, defining log storage and disposal requirements and roles and responsibilities for the log management infrastructure.	U	Assistant Administrator for Environmental Information	TBD		
4	8	Finalize the SIEM tool's "Enterprise Reference Guide."	O	Assistant Administrator for Environmental Information	3/29/13		
5	12	Issue a memorandum to OEI officials requiring the Senior Agency Information Officer be the addressee on all internal security reports and reviews in order to ensure identified weaknesses are recorded within the Agency's security weakness tracking system.	U	Assistant Administrator for Environmental Information	TBD		
6	12	Create POA&Ms for all recommendations applicable t Agency internal reports identified in Appendix B.	U	Assistant Administrator for Environmental Information	TBD		
7	12	Develop and implement a process to verify that identified weaknesses in Appendix B are addressed and decisions are documented on actions taken.	U	Assistant Administrator for Environmental Information	TBD		
8	12	Develop and implement a process to verify that regions and program office staff address vulnerabilities from NCC scans.	O	Assistant Administrator for Environmental Information	2/15/13		

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

EPA Monitoring Tools Reviewed

OEI manages EPA's IT infrastructure, supports EPA's information systems and information products, and develops strategies for information security. OEI management provided the OIG with a briefing on security tools used to secure the Agency's network infrastructure. The OIG also contacted EPA's regional information security community to determine whether they were using additional security tools to combat cyber-security events and monitor network traffic. The OIG learned that EPA regional offices in Kansas City, Kansas (Region 7), and Denver, Colorado (Region 8) were using log management tools to monitor network traffic. The OIG met with EPA personnel who managed those security tools to obtain information on each tool's functionalities, cost, and usage.

Table A-1 lists those security tools the OIG reviewed during this audit. The cost of each tool represents funds expended during fiscal years 2010 and 2011 to cover hardware and software requirements, training needs, annual maintenance and licenses.

Table A-1: **Security tools managed by EPA offices/regions visited**

Office\Region	Functionality	Cost
Office of Environmental Information/ Office of Technology Operations and Planning	Security incident and event management tool	$ 1,766,923
	eDiscovery and Forensic	974,495
	Virus protection software	614,547
	Patch management tool	453,166
	Netflow analyzer software	20,989
	Asset management tool	268,802
Region 7 (Kansas City Office)	Security audit log software	1,665
Region 8 (Denver Office)	Security incident and event management tool	42,032
Total		**$ 4,142,619**

Source: OIG analysis.

NCC personnel indicated that EPA's perimeter enforcement and web-filtering capabilities are managed through a U.S. General Services Administration services contract as part of a federal "cloud environment." EPA indicated that associated cost for this managed service is administered by the U.S. General Services Administration and costs specific to EPA could not be provided.

Unaddressed Recommendations

During 2009 and 2010, EPA conducted three separate internal reviews of the Agency's information security program: (1) Clampi Infection Lessons Learned, (2) CERT at Carnegie Mellon University Software Engineering Institute, and (3) Booz Allen Hamilton document for Mitigation of Advanced Persistent Threats**.**

OEI manages EPA's IT infrastructure, supporting the Agency's information systems and information products. OTOP also develops and implements IT policies, plans, and strategies for information security, investment management, and workforce training and development. TISS, within OTOP, is responsible for managing the Agency's IT security program; including IT security planning, program management, evaluation of effectiveness, support to other programs, support for policy and procedure development, and communications. TISS manages, oversees, and communicates the Agency's IT security program by providing a framework, tools, priorities and overall direction for EPA employees and management.

Background information on each document and the recommendations that remain unaddressed based on our audit work is detailed below.

Clampi Infection Lessons Learned

On July 10, 2009, EPA was infected with what appeared to be a Trojan horse virus. At 1:40 p.m., an initial report was received from Region 5 indicating 15 systems were infected. Seven minutes later, by 1:47 p.m., the infection was confirmed in Nevada, Virginia, North Carolina, Florida, and other locations across the nation. The infections were later identified as new variants of the Clampi Trojan. With the help of several stakeholders who were involved during this event, EPA created a lessons learned document in response to this event titled "Clampi Infection Lessons Learned" dated August 1, 2009. The document lists findings on what went well and areas of concern during the response to this event. Recommendations were addressed to the Computer Security Incident Response Capability (CSIRC) Center, Enterprise Desktop Solutions Division, Customer Technology Solutions (CTS), EPA Call Center, and the Senior Agency Information Security Officer.

Table B-1: **Findings and corresponding recommendations not addressed**

Finding(s) and applicable recommendation(s)	Responsible office for remediation
An ancillary finding to temporarily blocking webmail was that users are circumventing security controls and utilizing personal webmail to send and receive email on behalf of EPA. For example, in one ticket a user complained that she was no longer able to view her EPA mail on her iPhone because yahoo mail was blocked. Aside from a potential infection vector, sensitive EPA data could be lost, viewed, or stolen, should a user's personal account be compromised or personal device lost. 1. Set policy disallowing the use of personal webmail to conduct business on behalf of EPA. 2. Allow the viewing of personal webmail but filter the download of attachments. 3. If the fore-mentioned recommendations are operationally impossible, route third party webmail traffic through the demilitarized zone where it can be monitored for data leakage.	TISS
While the infection was ongoing, CSIRC struggled to locate the correct individuals for information. For example, we were unable to find the right person to provide a report on CTS Anti-Virus definitions. 1. Get an org. chart quarterly from CTS and ISOs.	CSIRC
Information briefly circulated indicating the Clampi Trojan was spreading via USB thumb drives. Although this was later proven false, the fact that EPA is vulnerable to infection from flash drives is true. 1. Disable autorun and autoplay. 2.Force virus scans on removable media.	Enterprise Desktop Solutions Division
EPA Call Center was overwhelmed with the influx of tickets. As the Clampi event wound to a close, CSIRC discovered events reported by CTS to the EPA Call Center that were never entered into Remedy by Apptis. 1. With two separate Remedy systems maintained and owned by separate vendors, confusion and duplicate tickets are a weekly occurrence. 2. We recommend automation between the systems or converging the two into one.	EPA Call Center
Several Regions/Program Offices were not represented on the emergency calls. 1. When a region/PO is unaccounted for during a national call, involve the IRM Branch Chiefs. ISOs stated they had no insight or influence over the CTS systems under their area of responsibility. Local site ISOs expressed displeasure that CTS didn't communicate with them. 2. Local ISOs need insight into all assets at their site. We recommend a dashboard for use by local ISOs with rollup to Primary ISOs for insight into their area of responsibility. 3. The ISOs role in security events needs to be more clearly defined. There is some confusion about CTS/CSIRC communicating directly with each other versus the ISO. ISOs without Blackberries did not find out about the Clampi infection until the next Monday. 4. Issue Blackberries to all ISOs. ISOs relying on contractor support ran into a problem where contractors were not approved to work overtime. 5. Set aside funding for emergency operations. ISOs complained the NSA toolkit was not useful and was introduced at the wrong time. 6. Continue the phased implementation and encourage ISOs to become familiar with the toolkit and its use.	Senior Agency Information Security Officer

Source: Clampi Infection Lessons Learned Document.

Carnegie Mellon Report

EPA entered into an engagement with the CERT Program at Carnegie Mellon University Software Engineering Institute to perform an appraisal of EPA's information security program based on CERT Resiliency Engineering Framework. Carnegie Mellon's report, *CERT Resiliency Engineering Framework, Environmental Protection Agency*, August 2009, identified several areas of improvements in EPA's incident response and handling program. Recommendations in Chapter 4 apply to the EPA's information security program as a whole.

Table B-2: **Findings and corresponding recommendations not addressed**

Finding/recommendation	Responsible office for remediation
Chapter 4 Appraisal Findings: Global Strengths and Weaknesses	
1. There is a dependence on heroic actions by individuals.	OTOP
2. Governance for information security activities is generally missing; however, Technology Management activities are receiving some governance from the Quality and Information Council/Quality Technology Subcommittee.	
3. There is a focus on tools as opposed to (and sometimes in conflict with) a focus on sound process and procedures.	
4. Information security program activities tend to be reactively evolved rather than proactively planned.	
5. The information security program is largely compliance-focused as opposed to requirements' driven.	
6. Information security metrics activities are lacking.	
7. People are accepting information security risks on behalf of the Agency who may not have the authority, necessary understanding or willingness to do so.	
8. There is a heavy reliance on contractors to perform critical functions in support of the Agency information security program without clear measures in place to ensure that program knowledge is sustainable.	
9. There is a lack of awareness and appreciation of information security activities in support of the Agency's business and mission.	
10. Manipulation of self-reported data has made internal and external compliance reports unreliable indicators of the Agency's information security posture.	
11. Agency management's focus on generating favorable internal and external reports has resulted in coaching respondents to adjust self-reported data to the detriment of the Agency's information security posture.	
12. Quality and validity of self-reported data is questionable and makes the enforcement and validation process difficult.	
13. Data calls to support compliance are numerous and often redundant.	
14. IT security money is allocated across Agency to support IT security responsibilities.	
15. Key information security roles (for example ISO, PO, IRO, ISSO, IMO, SA, and System owner) and their associated responsibilities are not well-defined, well-understood commonly captured in position descriptions, or well-aligned with training program.	
16. Agency management support for a consistent and repeatable information security program and process is lacking - current focus is reactive and compliance-driven.	
17. Enforcement actions related to information security are not enacted by Agency management.	

Finding/recommendation	Responsible office for remediation
Chapter 7 Appraisal Findings: Incident Management and Control (IMC) Capability area	
1. EPA seemed unclear on the processes that were to be followed relative to closing incidents including any lessons learned.	TISS
2. There was not sufficient evidence to suggest that lessons learned were being translated into actions to better protect Agency assets.	
3. There is no consistent or formalized process to identify recurring problems; examine root causes; or develop solutions for these problems with the goal of preventing future, similar incidents.	
Chapter 14 Recommendations: Prioritize and Address Capability Gaps	
1. Establish the internal procedures for incident management and control.	TISS
2. Establish procedures and criteria for the regular performance of post-incident reviews.	
3. Establish a link between the incident management and control process and the problems management process.	
4. Establish a process to improve asset protection and continuity strategies in response to lesson learned from managing incidents.	
5. Establish governance over the planning and performance of the incident management and control process.	
6. Establish and maintain the plan for performing the incident management and control process.	
7. Evaluate the sufficiency of incident management and control resources, and request resource changes as necessary.	
8. Formally assign responsibility and authority for performing the incident management and control process.	
9. Improve monitoring of the incident management and control process.	
10. Use appraisals or audits to objectively evaluate the adherence of the incident management and control activities to the process description, standards, and procedures.	

Source: Carnegie Mellon report.

Booz Allen Hamilton -Document

In August 2010, Booz Allen Hamilton was tasked to identify immediate and/or stop gap measures to protect EPA systems and data. Booz Allen Hamilton issued a document on November 5, 2010, on EPA's ability to mitigate Advanced Persistent Threats. Booz Allen Hamilton concluded that EPA had procedural and operational weaknesses preventing EPA from successfully mitigating Advanced Persistent Threats. Procedural weaknesses included areas such as governance, policy, procedures and oversight. Operational weaknesses included recommendations for implementing a risk mitigation program, sharing of forensic images by OIG, expanding CSIRC's mission and capabilities to address Advanced Persistent Threats across the enterprise, and obtaining/installing an enterprise event log aggregation/correlation tool.

Table B-3: **Findings and corresponding recommendations not addressed**

Finding/recommendation	**Responsible office for remediation**
Procedural Findings	
Ongoing senior management buy-in and support for the IT security program is essential 1. Identify senior management level of risk tolerance for IT Information Management assets.	TISS Senior Agency Information Security Officer
Strong governance around the IT security program is essential 2. Develop a formal agency governance program to oversee all IT security actions.	
IT security policies and procedures must be updated and current systems security verified 3. Perform an immediate review of all EPA IT security policies and procedures. 4. Based on senior management's risk tolerance, prioritize IT Information Management assets and validate security documentation.	
EPA is facing a challenge in its IT security environment that requires it to become more proactive in its actions, rather than reactive. Attackers will always be looking for the next gap. 5. Plan an Agency-wide cyber security program to identify and prioritize risks that impact the IT security program and design a risk management program across the offices and regions. 6. Include formal assessment and testing requirements in IT Information Management procurements to minimize introduction of new vulnerabilities and threats.	
EPA should consider innovative ways to improve IT security situational awareness. 7. Design a security awareness program that will more effectively drive the message to users.	
In accordance with NIST SP 800-39, EPA must adopt automated tools to achieve continuous monitoring for threats. 8. EPA needs to embrace a broader risk management perspective.	
EPA needs clear standards for training, roles, and responsibilities for IT Information Management security personnel. 9. Design a security awareness program that will more effectively drive the message to users. Consider the "think before you click" campaign concept. 10. Identify those who are most likely to be targeted based on position and access to information. Use available intelligence to identify what information is being targeted. Develop a security awareness program that is aimed specifically to this audience to promote their sensitization and awareness of accountability.	

Finding/recommendation	Responsible office for remediation
Actions by law enforcement or intelligence could act as a constraint to Incident Response actions, negatively impacting security or services. 11. Identify law enforcement and intelligence activity as a risk and engage in planning to determine a mitigation plan. Engage law enforcement and intelligence agencies in the mitigation planning.	TISS Senior Agency Information Security Officer
Operational Findings	
EPA does not have a risk mitigation program. 1. Deployment of specialized incident response tools as one element of the Proactive Threat Identification program. 2. Centralize efforts to identify all assets currently within the EPA enterprise and verify each has appropriate accreditation. 3. Designate personnel with the specific responsibility to identify and interact with those sources most likely to provide EPA with relevant data in the fastest time possible.	TISS
EPA's best practices to secure against IT threats are known. Mitigation, not elimination, can be achieved through the IT security program. 4. Focus the IT security program on detection, containment and eradication of threats.	
EPA is highly vulnerable to targeted/spear-phishing email. 5. EPA should consider a risk assessment related to information positioned in the public environment and assess the effects of the release, including the potential of creating targets for attackers within the Agency.	
CSIRC cannot readily determine as a compromised system is identified whether it belongs to a VIP or Senior Executive Staff. 6. Assess all users and identify those accounts most frequently in possession of, in communication with, that information EPA can't afford to lose.	
The EPA CSIRC program has been effective within its original function but is not capable of dealing with highly sophisticated Advanced Persistent Threat. 7. Expand CSIRC's mission and capabilities to address Advanced Persistent Threats across the enterprise. Obtain and install an enterprise event log aggregation/ correlation tool.	
Due to delegation of roles, all forensic images have been obtained by OIG and analysis/reporting is maintained close-hold. 8. The OIG should be encouraged to share that information that will improve security and not impact ongoing investigations. If copies of their images are not made available, the Agency should perform its own acquisition and forensic examination.	TISS

Source: Booz Allen Hamilton report.

Appendix C

Agency Response to Draft Report

9/06/2012

MEMORANDUM

SUBJECT: OEI's Response to OIG's Draft Report – Improvements Needed in EPA's Network Security Monitoring Program (OMS-FY11-0005)

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

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

In response to the draft Audit Report, "Improvements Needed in EPA's Network Security Monitoring Program" (OMS-FY11-0005), the Office of Environmental Information is pleased to provide you with our response to the OIG recommendations found in the report.

If you have any questions, please contact OEI Audit Follow-Up Coordinator, Scott Dockum at 202-566-1914.

Attachment

cc: James McDonald
Robbie Young
Scott Dockum
Elizabeth Braziel

Office of Environmental Information / OTOP
Corrective Action Plan

Auditing Group: OIG **Audit No.:** OMS-FY11-0005	**Audit Title:** Improvements Needed in EPA's Network Security Monitoring Program
Report Date: August 7, 2012 **OEI Lead Offices:** OTOP & SAISO	**OEI Leads and Phone:** OTOP - Anne Mangiafico 202-564-9483; SAISO – Robert McKinney (202) 564-0921

Recommendation	Corrective Action	Planned Completion Date	Status	POC for Recommendation	Comments	Concur Yes/No
1: Develop and implement a strategy with milestone dates to incorporate EPA's headquarters program offices within the SIEM environment.	TISS will refine the project plan to reflect a thorough strategy for incorporating Program Offices into the SIEM environment. This strategy will include milestone dates for all Program Offices not already in SIEM.	12/31/13	In Progress - Implementing Program Office devices into ArcSight is currently underway as part of the overall strategy. A project plan exists that lists each Program Office.	OTOP/TISS Lee Kelly	There are multiple Program Offices already in ArcSight. Along with the Regional offices, other Program Offices are in various stages (Initial contact; Information Gathering; Testing; etc.) regarding implementation.	Yes
2: Develop and implement a formal training program that will meet EPA's information security	TISS will further codify the training program for ArcSight by documenting evidence of training	12/31/12	In Progress – A user guide has been developed and made available to	OTOP/TISS Lee Kelly	Training on ArcSight is accomplished in various methods. (1) Upon being	Yes

staff needs in using the SIEM tool. The training program should include a user guide on using the SIEM tool to generate reports and developing customized reports for filtering known and suspicious events.	for users and formalizing training requirements for ArcSight access.		users. Efforts moving forward will focus on refining the user guide and formalizing the training program.		granted access to ArcSight a one-on-one session is scheduled with the user to go over the interface, basic/advanced searches, reports (default and custom) and queries among other items. This session usually lasts between 60-90 minutes; (2) Hewlett Packard (ArcSight manufacturer) also provides training courses on ArcSight on a fee-based schedule available from their website. (3) At the bi-weekly ArcSight user group meeting demonstrations are held on how to perform certain functions and the users have an opportunity to ask	

					questions on that topic. A user guide that includes chapters on reports and searches has been posted to the EPA SIEM collaboration page. This information was announced at the last user group meeting.	
3: Develop a policy or revise the Agency's Information Security Policy to comply with NIST SP 800-92. This policy should include, but not be limited to, defining log storage and disposal requirements and roles and responsibilities for the log management infrastructure.	The SAISO will review the Agency's Information Security Policy/Procedure to comply with NIST SP 800-92 and revise if necessary.	TBD				Yes
4: Finalize the SIEM tool's "Enterprise Reference Guide."	The Enterprise Reference Guide will be reviewed to determine gaps between its guidance and the current status of the SIEM project. The Enterprise	3/29/13	In Progress	OTOP/TISS Lee Kelly		Yes

	Reference Guide will be updated and finalized, and referenced in other TISS/CSIRC operating procedures if necessary.					
5: Appoint in writing a central point of contact for tracking the completion of weaknesses discovered during internal assessments.	The SAISO is currently responsible in accordance with FISMA as the central point of contact for tracking weaknesses. OTOP/NCC will appoint in writing a central point of contact for tracking the completion of weakness discovered during internal assessments.	TBD				No
6: Create POA&Ms for all recommendations applicable to Agency internal reports identified in Appendix B.	The SAISO will create POA&Ms for all applicable recommendations to Agency internal reports identified in Appendix B.	TBD				Yes
7: Develop and implement a process to verify that identified weaknesses in Appendix B are addressed and	The SAISO will develop an enhanced process model for the full life cycle management of Plans	TBD				Yes

decisions are documented on actions taken.	of Actions and Milestones (POA&M) resulting from identified weaknesses of the Agency Information Security Program.					
8: Develop and implement a process to verify that regions and program office staff address vulnerabilities from NCC scans.	OTOP/NCC will revise the agency's vulnerability management standard operating procedure (SOP) to incorporate a verification process to ensure regions and program offices are appropriately addressing vulnerabilities from NCC scans. The revised SOP is contingent upon OEI CIO approval/signature of the "Information Security Interim Roles and Responsibilities Procedures" document currently in process.	2/15/2013	On-going	OTOP/NCC John Gibson	Review of new EPA Infosec Policy will be required	Yes

During the OIG exit conference September 12, 2012, it was agreed that recommendation # 5 was to be amended as follows.

5 (Amended) New text Issue a memorandum to OEI officials requiring the SAISO be the addressee on all internal security reports and reviews in order to ensure identified weaknesses are recorded within the Agency's security weakness tracking system.	SIASO will issue a memo to OEI officials.	TBD	Ongoing	SAISO		Yes

Appendix D

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information and Chief Information Officer
Senior Agency Information Security Officer, Office of Environmental Information
Director, Office of Technology Operations and Planning, Office of Environmental Information
Acting Director, Enterprise Desktop Solutions Division, Office of Environmental Information
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 External Affairs and Environmental Education
Audit Follow-Up Coordinator, Office of Environmental Information
Audit Follow-Up Coordinator, Office of Technology Operations and Planning,
    Office of Environmental Information
Audit Follow-Up Coordinator, Technology and Information Security Staff,
    Office of Environmental Information