U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

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

Report No. 09-P-0240

September 21, 2009

Report Contributors:

Rudolph M. Brevard
Charles M. Dade
Jefferson Gilkeson
Teresa Richardson
Cory Costango
Scott Sammons

Abbreviations

ASSERT	Automated Security Self-Evaluation and Remediation Tracking
BRAINS	Billing and Reimbursable Accounting Network System
EPA	U.S. Environmental Protection Agency
IT	Information Technology
mLINQS	Relocation Expense Management System
NIST	National Institute of Standards and Technology
NTSD	National Technology Services Division
OARM	Office of Administration and Resources Management
OCFO	Office of the Chief Financial Officer
OEI	Office of Environmental Information
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&Ms	Plans of Action and Milestones
VMP	Vulnerability Management Program

U.S. Environmental Protection Agency
Office of Inspector General

09-P-0240
September 21, 2009

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

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

Background

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

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

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

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

What We Found

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

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

What We Recommend

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

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

The Agency agreed with all of our findings and recommendations.

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

OFFICE OF
INSPECTOR GENERAL

September 21, 2009

MEMORANDUM

SUBJECT: Project Delays Prevent EPA from Implementing an Agency-wide Information Security Vulnerability Management Program
Report No. 09-P-0240

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

TO: Linda A. Travers
Acting Assistant Administrator and Chief Information Officer
Office of Environmental Information

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

The estimated cost of this report – calculated by multiplying the project's staff days by the applicable daily full cost billing rates in effect at the time – is $475,431.

Action Required

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

If you or your staff have any questions regarding this report, please contact me at 202-566-0893 or brevard.rudy@epa.gov; or Charles M. Dade, Project Manager, at 202-566-2575 or dade.chuck@epa.gov.

Table of Contents

Purpose 1

Background 1

Noteworthy Achievements 1

Scope and Methodology 2

Other Reporting Matters 2

Results of Review 3

Lack of a Vulnerability Management Tool Inhibits EPA's Ability to Continuously Monitor Its Network Resources 3

Vulnerability Management Project Needs an Interim Solution and Stakeholder Involvement 4

Recommendations 5

Agency Comments and OIG Evaluation 6

Status of Recommendations and Potential Monetary Benefits 7

Appendices

A **Status of Agreed-to Recommendations** 8

B **Status of Unimplemented Recommendations** 9

C **Agency Response to Draft Audit Report** 17

D **Distribution** 19

Purpose

We sought to evaluate the implementation and effectiveness of the Agency's corrective actions for prior information security audit recommendations.

Background

Implementing corrective actions to resolve issues is essential to improving the efficiency and effectiveness of U.S. Environmental Protection Agency (EPA) operations. Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*, requires that managers take timely and effective action to correct issues identified by a variety of sources. Office of Inspector General (OIG) audit reports represent one such source. OMB Circular A-123 also requires management to show that corrective actions taken achieve the desired results. It also specifies that the results achieved should be documented in writing. Further, supporting documentation should be available for review. OMB Circular A-123 states that correcting issues is an integral part of management accountability and must be considered a priority by the Agency.

EPA has policies to guide managers when implementing audit recommendations. Specifically, EPA Manual 2750, *EPA Audit Management Process*, provides timeframes for audit resolution. It also requires that EPA action officials create systems to ensure that recommendations are implemented. EPA Order 1000.24, *Management Integrity*, states that weaknesses should be corrected at the organizational level closest to the problem. Further, it states that weaknesses should be dealt with as soon as possible after being identified.

We chose four audit reports to determine whether the Agency has taken action to correct information security weaknesses identified in each of them (see Table 1).

Table 1: Prior Audits Reviewed Regarding Information Security Weaknesses

Report No.	Report Title	Date
2004-P-00013	*EPA's Administration of Network Firewalls Needs Improvement*	March 31, 2004
2005-P-00011	*Security Configuration and Monitoring of EPA's Remote Access Methods Need Improvement*	March 22, 2005
2007-P-00007	*EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents*	January 11, 2007
08-1-0032	*Audit of EPA's Fiscal 2007 and 2006 (Restated) Consolidated Financial Statements* (only reviewed recommendations made to improve information security)	November 15, 2007

Source: OIG analysis

Noteworthy Achievements

EPA has taken steps to strengthen network security by implementing an appliance-based firewall server that meets an industry standard architecture. EPA also updated its incident-reporting directive to include new roles, responsibilities, and standards for centralized incident reporting.

Scope and Methodology

We performed our audit from January 2008 to June 2009. We performed this audit in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient and appropriate evidence. The evidence is to provide a reasonable basis for our findings and conclusions. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

We compared EPA's written assertions of the status of agreed-to report recommendations with documentary support of the actions EPA took. We also spoke with EPA and contractor staff in the Office of Environmental Information (OEI) and the Office of Administration and Resources Management (OARM) responsible for implementing and overseeing actions to address the related audit recommendations. We identified actions EPA still needed to take to fully satisfy each recommendation.

We spoke with EPA and contractor staff in the Office of Air and Radiation, Office of Research and Development, OARM, and EPA Regions 4 and 5. We asked about system control monitoring practices of Web-Mail-enabled servers. We asked about practices, methods, and tools these sites use to detect and protect their networks against vulnerabilities. During visits to EPA regional offices for Regions 4 and 5, we performed vulnerability tests on selected application servers that allow remote access to EPA's electronic mail system. We provided the test results to the regional staff for resolution. We spoke with OEI and OARM audit follow-up coordinators, as well as EPA line staff who implement corrective actions. These individuals determine whether their offices have processes in place to evaluate the effectiveness of those actions.

Other Reporting Matters

During preliminary research, we issued a memorandum to EPA's Chief Financial Officer on the status of actions taken to correct information security weaknesses at the Cincinnati Finance Center. The Office of the Chief Financial Officer (OCFO) took ample steps to correct material weaknesses in physical access and environmental controls at the Cincinnati Finance Center. However, OCFO still needed to do more work to document and test security controls over the two critical applications at the finance center. The OIG reviewed EPA's progress in completing these remaining recommendations during the Fiscal Year 2008 financial statement audit. In examining that audit, we found that the Agency made significant progress in completing the agreed-to corrective actions, but it still needs to finalize the independent reviews of the two financial applications and update the applications' security plans. In addition, the Agency needs to test the newly approved contingency plans for these two applications.

Also during preliminary research, we provided OCFO with written comments directing it to strengthen EPA Manual 2750 and EPA Order 1000.24. We found that EPA needed to update EPA Manual 2750 to more clearly assign responsibility for ensuring corrective actions are effective and implemented in a timely manner, as required by OMB Circular A-123. We found that internal controls for overseeing corrective actions defined in EPA Order 1000.24 needed updating to specify something to this effect: "A determination that a weakness has been

corrected is made only when management demonstrates that the corrective action taken effectively resolved the identified weakness."

Appendix A provides the status of agreed-upon recommendations for the four reports we reviewed. Appendix B provides information on all open agreed-to recommendations that still require EPA management action to complete.

Results of Review

EPA made progress in implementing many of the agreed-upon audit recommendations. However, more management emphasis is needed to complete a key project that would provide EPA offices with the necessary tools to continuously monitor their network resources. In particular, since 2005, EPA has attempted to implement a commercial off-the-shelf network vulnerability tool. This tool has the capability to identify and correct commonly known security weaknesses. However, project delays have thwarted EPA's ability to move the project beyond the pilot stage. As a result, EPA regional and program offices are inconsistent in routinely monitoring their networks for common vulnerabilities. Offices that do routinely monitor their networks for common vulnerabilities use inconsistent methods.

Lack of a Vulnerability Management Tool Inhibits EPA's Ability to Continuously Monitor Its Network Resources

EPA has not established an Agency-wide security-monitoring program for its computer network. Significant delays have occurred in completing the information technology (IT) project related to this effort. In our 2004 audit of EPA's network firewall and our 2005 audit of remote access methods, we recommended that EPA:

- Modify the network vulnerability assessment methodology to include scanning of all firewall components.

- 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.

- Expand the Agency's security-monitoring program to include using a variety of network vulnerability scanning tools to monitor registered servers.

- Establish and implement a process to ensure program and regional offices conduct regular security monitoring that includes vulnerability scanning.

Completing these recommendations called for EPA to implement a vulnerability management program (VMP). In July 2005, EPA began to establish the program. Yet, more than 3 years later, EPA is still evaluating a vulnerability management tool. The Research Triangle Park campus and an EPA region served as the two pilot sites for testing the selected tool. OEI staff mentioned that it is necessary to automate both the vulnerability detection and remediation processes before rolling out the vulnerability management tool for EPA locations to use.

Automating only the detection process would overwhelm EPA IT security staff because they would have to manually remediate vulnerabilities. We agree with the Agency that remediating vulnerabilities would initially increase the workload of EPA IT security staff. However, this increase in workload would decrease over time once the Agency becomes more familiar with the vulnerability management tool. We believe this short-term increase in workload would put EPA in a better position to more quickly remediate high risk vulnerabilities and provide better protection of critical network resources once a vulnerability remediation process is in place. National Institute of Standards and Technology (NIST) Special Publication 800-123, *Guide to General Server Security*, states that scanning should occur on a weekly to monthly basis. NIST stresses that this ongoing scanning is extremely important for mitigating vulnerabilities as soon as possible to prevent vulnerabilities from being discovered and exploited.

Vulnerability Management Project Needs an Interim Solution and Stakeholder Involvement

As OEI progressed with the project, automating the remediation process became increasingly difficult. With the exception of common network services, EPA operates a decentralized managed network. Hardware and software component configurations vary by EPA location. Calibrating a vulnerability management tool that can remediate vulnerabilities on a variety of hardware and software configurations across EPA's decentralized network presents a major challenge. As such, providing an interim solution to identify vulnerabilities until an automated solution is available would provide EPA offices with:

- A consistent approach to monitoring their networks continuously.
- A means to provide feedback to help configure the automated remediation component of the VMP.
- A means to transition to new vulnerability management components when they become available.

Further, establishing a formal centralized oversight structure would help ensure that management has in place a repeatable and documented practice. This practice would provide much needed consistency and structure to network vulnerability testing and remediation. However, EPA did not provide offices with an interim solution for conducting continuous monitoring of their network resources. During our visits to five EPA offices, we confirmed that they do not regularly and consistently test their networks for vulnerabilities.

We asked employees involved in the project about this and other issues that were delaying the project's completion. We requested information on actions taken by EPA to address these issues. We further asked for the planned project completion date, project budget data, and status of key milestones. However, as of August 6, 2009, EPA management had not provided the information related to our request.

In addition, during interviews with EPA employees involved in the project, it came to our attention that conditions existed that suggest management could have taken more steps to prepare stakeholders for the new VMP. For example, the Project Manager indicated that EPA management did not establish a workgroup composed of key stakeholders from the various EPA

programs and regional offices. Also, IT security personnel who were involved in the pilot indicated they would need to receive additional training to ease the implementation of the vulnerability management program associated with this project.

As of August 6, 2009, EPA provided a partial work plan, which included only the pilot phase of the project, to implement an Agency-wide VMP. A review of this work plan shows that EPA planned to complete the pilot phase of this project in February 2009. Nevertheless, the work plan does not provide information on when EPA plans to have an Agency-wide VMP in place. As of August 6, 2009, EPA did not provide information on the steps it took to address the delays in implementing the VMP.

As a result of our audit, OEI issued a memorandum on August 3, 2009, to remind applicable Agency personnel of their vulnerability scanning/remediation responsibilities and to point them to available resources to assist in fulfilling these responsibilities. However, the information and documentation referenced within the memorandum needs to be revised to reflect the latest revision of NIST Special Publication 800-53, as well as the latest minimum standard for time between the periodic vulnerability scanning/remediation. The memorandum indicated that the time between periodic vulnerability scanning and remediation is not to exceed one quarter. However, NIST guidance states that scanning should occur on a weekly to monthly basis. Additionally, NIST also states periodic scans should be performed using two different tools because no scanner is able to detect all known vulnerabilities.

Additionally, although the memorandum references available resources to assist Agency personnel in fulfilling their vulnerability scanning/remediation responsibilities, OEI made disclaimer statements regarding licensing limitations and resource availability associated with the resources/tools they were offering. We believe this disclaimer indicates a lack of management commitment and support for establishing an effective vulnerability management program within EPA.

Due to the datedness and vagueness of the memorandum and the lack of resources and necessary licenses for the tools implied by the disclaimer, we added Recommendation 5 to the "Recommendations" section below.

Recommendations

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

1. Create Plans of Action and Milestones (POA&Ms) for each unimplemented audit recommendation listed in Appendix B.

2. Update EPA's Management Audit Tracking System to show the status of each unimplemented audit recommendation listed in Appendix B.

3. Provide EPA program and regional offices with an interim solution for vulnerability management. This should include establishing a centralized oversight process to

ensure that EPA program and regional offices (a) regularly test their computer networks for vulnerabilities, and (b) maintain files documenting the mitigation of detected vulnerabilities.

4. Establish a workgroup of program and regional EPA IT staff (e.g., information security officers, system administrators, etc.) to solicit input on training needs and facilitate the rollout of the Agency-wide vulnerability management program.

5. 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.
    d. Specifies what tools and resources OEI can actually provide to help the applicable personnel fulfill these responsibilities and what the applicable organizations will have to obtain on their own to perform these responsibilities.

Agency Comments and OIG Evaluation

Within its July 30, 2009, response to the draft report, OEI agreed with the findings and recommendations. OEI did not provide an updated status on the recommendations identified in Appendix B with their response. We added an additional column to the end of Appendix B in which we included the information we obtained from the Automated Security Self-Evaluation and Remediation Tracking (ASSERT) system as of August 6, 2009. However, OEI indicated it would create POA&Ms for all of the report's recommendations.

Appendix C contains the Agency's complete response to our formal draft 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	5	Create Plans of Action and Milestones (POA&Ms) for each unimplemented audit recommendation listed in Appendix B.	O	Director, Office of Technology Operations and Planning, within the Office of Environmental Information			
2	5	Update EPA's Management Audit Tracking System to show the status of each unimplemented audit recommendation listed in Appendix B.	O	Director, Office of Technology Operations and Planning, within the Office of Environmental Information			
3	5	Provide EPA program and regional offices with an interim solution for vulnerability management. This should include establishing a centralized oversight process to ensure that EPA program and regional offices (a) regularly test their computer networks for vulnerabilities, and (b) maintain files documenting the mitigation of detected vulnerabilities.	O	Director, Office of Technology Operations and Planning, within the Office of Environmental Information			
4	6	Establish a workgroup of program and regional EPA IT staff (e.g., information security officers, system administrators, etc.) to solicit input on training needs and facilitate the rollout of the Agency-wide vulnerability management program.	O	Director, Office of Technology Operations and Planning, within the Office of Environmental Information			
5	6	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. d. Specifies what tools and resources OEI can actually provide to help the applicable personnel fulfill these responsibilities and what the applicable organizations will have to obtain on their own to perform these responsibilities.	O	Director, Office of Technology Operations and Planning, within the Office of Environmental Information			

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

Appendix A

Status of Agreed-to Recommendations

Report Title/Number	Recommendation Number	Recommendations Completed	
		Yes	No
EPA's Administration of Network Firewalls Needs Improvement (Report No. 2004-P-00013)	2-1		X
	3-1	X	
	3-2		X
Security Configuration and Monitoring of EPA's Remote Access Methods Need Improvement (Report No. 2005-P-00011)	2-1		X
	2-2		X
	2-3		X
	2-4		X
	2-5		X
	3-1	X	
	3-2	X	
EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents (Report No. 2007-P-00007)	2-1		X
	2-2	X	
	2-3	X	
	3-1	X	
	3-2	X	
	3-3	X	
	3-4	X	
Audit of EPA's Fiscal 2007 and 2006 (Restated) Consolidated Financial Statements (Report No. 08-1-0032)	12		X
	13		X
	14	X	
	15		X
	16	X	
	17	X	
	18		X
	19	X	
	20	X	
	21	X	
Number Completed/Not Completed		**15**	**12**
Percentage Completed/Not Completed		**56%**	**44%**

Source: OIG analysis

Appendix B

Status of Unimplemented Recommendations

Report Title/Number	Recommendation	Action Needed	Requested Updated Status from Agency – Agency Provided No Updated Status as of June 23, 2009	ASSERT POA&M Information as of August 6, 2009
EPA's Administration of Network Firewalls Needs Improvement (Report No. 2004-P-00013)	2-1 Develop and implement a standard configuration requirement for adequately securing workstations used to remotely administer network firewalls.	Complete the implementation of "proxy" servers for remote access to firewall consoles. Management approval and issuance of the procedure developed for granting access to firewall consoles.	Planned implementation date for both actions was August 2008. As of February 9, 2009, EPA updated the POA&M in the ASSERT system with a new completion date of March 31, 2009.	The POA&M in ASSERT indicates that this Milestone Status is Completed. The OMB Comment does not appear to corroborate the milestone status. The OMB Comment states that the review was completed and modifications are being made to access methods based on outcome.
	3-2 Modify the network vulnerability assessment methodology to include scanning of all firewall components (e.g., workstations, management consoles, and enforcement point servers).	Implement regular vulnerability scanning of security infrastructure.	Planned implementation date was September 2008. As of February 9, 2009, EPA updated the POA&M in the ASSERT system with a new completion date of March 31, 2009.	Current revised completion date is September 30, 2009.

Report Title/Number	Recommendation	Action Needed	Requested Updated Status from Agency – Agency Provided No Updated Status as of June 23, 2009	ASSERT POA&M Information as of August 6, 2009
Security Configuration and Monitoring of EPA's Remote Access Methods Need Improvement (Report No. 2005-P-00011)	2-1 Establish processes and assign accountability for independently verify and validate that Web-Mail and BlackBerry servers comply with published EPA policies and standards.	Put formal processes in place and formally assign accountability for independently verifying and validating that Web-Mail servers comply with published EPA policies and standards.	**EPA management has not provided a complete project plan that includes the actions to be taken and the estimated or planned milestone dates for completing the actions necessary to address the recommendation.** Implementation date depends on the results of the ongoing vulnerability management pilot program. Based on a May 2008 interview with the project's technical lead, the planned completion date for the pilot program is March 2009.	Current revised completion date is August 31, 2009.

Report Title/Number	Recommendation	Action Needed	Requested Updated Status from Agency – Agency Provided No Updated Status as of June 23, 2009	ASSERT POA&M Information as of August 6, 2009
	2-2 Develop and implement a security-monitoring program that includes testing all servers, and require all system administrators to register their servers with NTSD and participate in the security-monitoring program.	Implement an Agency-wide vulnerability management program that includes registering and testing all servers on a regular basis (in compliance with Federal and Agency Regulations, Policies, Procedures, and Standards), remediating the vulnerabilities in a timely manner.	**EPA management has not provided a complete project plan that includes the actions to be taken and the estimated or planned milestone dates for completing the actions necessary to address the recommendation.** Implementation date depends on the results of the ongoing vulnerability management pilot program. Based on a May 2008 interview with the project's technical lead, the planned completion date for the pilot program is March 2009.	Current revised completion date is August 31, 2009.

Report Title/Number	Recommendation	Action Needed	Requested Updated Status from Agency – Agency Provided No Updated Status as of June 23, 2009	ASSERT POA&M Information as of August 6, 2009
	2-3 Expand the Agency's security-monitoring program to include using a variety of network vulnerability scanning tools to monitor registered servers.	Implement processes and utilize tools to support Agency-wide vulnerability scanning of critical network.	**EPA management has not provided a complete project plan that includes the actions to be taken and the estimated or planned milestone dates for completing the actions necessary to address the recommendation.** Implementation date depends on the results of the ongoing vulnerability management pilot program. Based on a May 2008 interview with the project's technical lead, the planned completion date for the pilot program is March 2009.	Current revised completion date is August 31, 2009.

Report Title/Number	Recommendation	Action Needed	Requested Updated Status from Agency – Agency Provided No Updated Status as of June 23, 2009	ASSERT POA&M Information as of August 6, 2009
	2-4 Establish and implement a process to ensure program and regional offices conduct regular security monitoring that includes vulnerability scanning.	Establish and implement a process to ensure program and regional offices conduct regular security monitoring that includes vulnerability scanning.	**EPA management has not provided a complete project plan that includes the actions to be taken and the estimated or planned milestone dates for completing the actions necessary to address the recommendation.** Implementation date depends on the results of the ongoing vulnerability management pilot program. Based on a May 2008 interview with the project's technical lead, the planned completion date for the pilot program is March 2009.	Current revised completion date is August 31, 2009.
	2-5 Develop and publish standards that define authorized open ports and services for the Web-Mail and BlackBerry servers' Operating System.	Develop and publish standards that define authorized open ports and services for the Web-Mail and BlackBerry servers' Operating System and require Web-mail and BlackBerry servers to be single-purpose servers.	EPA has not provided a planned implementation date for the corrective actions associated with this recommendation.	EPA has not established a POA&M to address this recommendation.

Report Title/Number	Recommendation	Action Needed	Requested Updated Status from Agency – Agency Provided No Updated Status as of June 23, 2009	ASSERT POA&M Information as of August 6, 2009
EPA Could Improve Processes for Managing Contractor Systems and Reporting Incidents (Report No. 2007-P-00007)	2-1 Develop and implement guidance that EPA offices can use to identify contractor systems that contain EPA data.	Update Information Security Manual to include procedures EPA offices can use to identify contractor systems that contain EPA data.	Planned implementation date for both actions was September 18, 2008. As of February 9, 2009, EPA updated the POA&M in the ASSERT system with a new planned completion date of April 10, 2009.	The POA&M in ASSERT indicates that this Milestone Status is completed as of June 30, 2009. The OMB Comment does not corroborate the milestone status. The OMB Comment states that contractual and resource ability to review draft documents have delayed this activity.
Audit of EPA's Fiscal 2007 and 2006 (Restated) Consolidated Financial Statements (Report No. 08-1-0032)	12 Develop a contingency plan for BRAINS and mLINQS. The plans should be approved by management and have documented annual reviews and testing.	Conduct a test of the two newly developed contingency plans.	As of the end of the Fiscal Year 2008 financial statement audit, EPA had not completed the corrective actions associated with this recommendation. The OIG will track EPA's progress in completing this recommendation during the annual financial statement audit.	The OIG will track EPA's progress in completing this recommendation during Fiscal Year 2009's annual financial statement audit.

Report Title/Number	Recommendation	Action Needed	Requested Updated Status from Agency – Agency Provided No Updated Status as of June 23, 2009	ASSERT POA&M Information as of August 6, 2009
	13 Develop a security plan for BRAINS and mLINQS. This should include having both applications comply with all the federal security requirements specified by the National Institute for Standards and Technology, including completion of the security certification and accreditation process and the resulting formal authorization to operate.	Finalize the independent reviews and updated security plans.	As of the end of the Fiscal Year 2008 financial statement audit, EPA had not completed the corrective actions associated with this recommendation. The OIG will track EPA's progress made in completing this recommendation during the annual financial statement audit.	The OIG will track EPA's progress in completing this recommendation during Fiscal Year 2009's annual financial statement audit.
	15 Enter Plans of Action and Milestones for all the above noted deficiencies in the Agency's security weakness tracking database (ASSERT).	Update ASSERT as POA&Ms change.	As of the end of the Fiscal Year 2008 financial statement audit, EPA had not completed the corrective actions associated with this recommendation. The OIG will track EPA's progress in completing this recommendation during the annual financial statement audit.	The OIG will track EPA's progress in completing this recommendation during Fiscal Year 2009's annual financial statement audit.

Report Title/Number	Recommendation	Action Needed	Requested Updated Status from Agency – Agency Provided No Updated Status as of June 23, 2009	ASSERT POA&M Information as of August 6, 2009
	18 Conduct and document an annual verification and validation of implemented procedures to ensure controls are implemented as intended and are effective.	Conduct and document an annual verification and validation of implemented procedures to ensure controls are implemented as intended and are effective.	As of the end of the Fiscal Year 2008 financial statement audit, EPA had not completed the corrective actions associated with this recommendation. Based on EPA Management's October 2008 response, EPA set December 31, 2008, as the implementation date for this recommendation. The OIG will track EPA's progress in completing this recommendation during the annual financial statement audit.	The OIG will track EPA's progress in completing this recommendation during the Fiscal Year 2009 financial statement audit.

Appendix C

Agency Response to Draft Audit Report

Jul 30, 2009

MEMORANDUM

SUBJECT: Response to Draft Audit Report Project No. OMS-FY08-0001, Project Delays Prevent EPA from Implementing an Agency-Wide Vulnerability Management Program

FROM: Vaughn Noga, Acting Director
Office of Technology Operations and Planning
and Acting Chief Technology Officer

TO: Rudolph M. Brevard, Director
Information Resources management Assessments
Office of Inspector General

We have completed our review of the OIG Draft Audit Report Project No. OMS-FY08-0001, *Project Delays Prevent EPA from Implementing an Agency-Wide Vulnerability Management Program* and are providing the following comments to your recommendations:

1. Recommendation #1 – Create Plans of Action and Milestones for each unimplemented audit recommendation listed in Appendix B.

   Concur in part – Many of the unimplemented audit recommendations have been assigned Plan of Action and Milestones (POA&Ms). For those recommendations that have not been assigned POA&Ms, OEI will ensure they have been created. Additionally, OEI will update its POA&Ms to reflect the milestones being identified in our current process improvement planning activities. Estimated date of completion for initial planning is August 31, 2009.

2. Recommendation #2 – Update the EPA's Management Audit Tracking System to show the status of each unimplemented audit recommendation listed in Appendix B.

   Concur – OEI will ensure EPA's Management Audit Tracking System (MATS) is updated to show the status of each agreed upon, unimplemented audit recommendation under its purview with in the limitations of the system. OEI recommends that OIG continue to utilize the Automated System Security Evaluation and Remediation Tracking (ASSERT) system to monitor status as MATS will be updated with the ASSERT POA&M Task ID.

3. Recommendation #3 – Provide EPA Program and Regional offices with an interim solution for vulnerability management. This should include establishing a centralized oversight process to ensure that EPA Program and Regional offices (1) regularly test their computer networks for vulnerabilities, and (2) maintain files documenting the mitigation of detected vulnerabilities.

   Concur – OEI will issue a memorandum to all Senior Information Officials, Information Management Officials and Information Security Officers reminding them of their responsibilities in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-53 to periodically scan systems for vulnerabilities on a continuous basis, implement appropriate remedial actions and what Agency and non-Agency tools available/recommended for use e.g. the Test and Vulnerability Assessment Lab (TVAL) and Nessus Vulnerability Scanner.

   Additional oversight and compliance will be conducted on a continuous basis via the Technology and Information Security Staff (TISS) Independent Verification and Validation (IV&V) activities.

4. Establish a workgroup of program and regional EPA IT staff (e.g., information security officers, system administrators etc.) to solicit input on training needs and to facilitate the rollout of the Agency-wide vulnerability management program.

   Concur – OEI will charter and manage a Patch and Vulnerability Group (PVG) in accordance with NIST SP 800-40. This group will conduct a variety of functions in support of the EVMP to include, but not limited to, identifying and ensuring the implementation of role-based training requirements to appropriate Information Technology (IT) personnel.

Thank you for giving us the opportunity to provide responses on this report. If there are any questions concerning the provided information please contact Johnny E. Davis Jr. at 202-566-1025.

cc: Johnny E. Davis Jr.
Robin Gonzalez
Bill Boone

Appendix D

Distribution

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