U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Special Report

Fiscal Year 2009 Federal Information Security Management Act Report

Status of EPA's Computer Security Program

Report No. 10-P-0030

November 18, 2009

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

OFFICE OF
INSPECTOR GENERAL

November 18, 2009

MEMORANDUM

SUBJECT: Fiscal Year 2009 Federal Information Security Management Act Report: Status of EPA's Computer Security Program
Report No. 10-P-0030

FROM: Bill A. Roderick
Deputy Inspector General

TO: Lisa P. Jackson
Administrator

Attached is the Office of Inspector General's (OIG's) Fiscal Year 2009 Federal Information Security Management Act (FISMA) Reporting Template, as prescribed by the Office of Management and Budget (OMB). Williams, Adley and Company, LLP, performed this review under the direction of the U.S. Environmental Protection Agency's OIG and performed the review in accordance with generally accepted government auditing standards. These standards require them to plan and perform the review to obtain sufficient and appropriate evidence to provide a reasonable basis for their findings and conclusions based on the objectives of the review.

Williams, Adley, and Company, LLP, limited their testing to those managerial controls necessary to achieve the objectives described in OMB Memorandum M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, August 20, 2009. Williams, Adley, and Company, LLP, did not test all managerial controls relevant to the effectiveness of the Agency's information security program as broadly defined by FISMA.

We believe the evidence obtained provides a reasonable basis for our findings and conclusions, and in all material respects meets the FISMA reporting requirements prescribed by OMB. In accordance with OMB reporting instructions, I am forwarding this report to you for submission, along with the Agency's required information, to the Director, OMB.

Furthermore, OIG audit work performed during Fiscal Year 2009 did not disclose material weaknesses with respect to the Agency's information security program that should be disclosed

pursuant to the Federal Managers' Financial Integrity Act of 1982. However, OIG audits noted significant weaknesses with several aspects of EPA's information security program. Appendix A synopsizes the results of our significant Fiscal Year 2009 information security audits.

The estimated cost for performing this audit, which includes contract costs and OIG contract management oversight, is $164,271.

Inspector General

Section Report

Environmental Protection Agency

Question 1: FISMA Systems Inventory & Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

1. Identify the number of Agency and contractor systems by component and FIPS 199 impact level (low, moderate, high) reviewed.

2. For the Total Number of Reviewed Systems Identified by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						Question 2		
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems(Agency and Contractor systems)		a. Number of systems certified and accredited	b. Number of systems for which security controls have been tested and reviewed in the past year	c. Number of systems for which contingency plans have been tested in accordance with policy
Agency/Component	Category	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed			
OA	High	0	0	0	0	0	0	0	0	0
	Moderate	0	0	0	0	0	0	0	0	0
	Low	2	1	0	0	2	1	1	1	1
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	2	1	0	0	2	1	1	1	1
OAR	High	1	0	0	0	1	0	0	0	0
	Moderate	9	1	1	0	10	1	1	1	1
	Low	3	0	1	0	4	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	13	1	2	0	15	1	1	1	1

Question 1: FISMA Systems Inventory & Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

		Question 1						Question 2		
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems(Agency and Contractor systems)		a. Number of systems certified and accredited	b. Number of systems for which security controls have been tested and reviewed in the past year	c. Number of systems for which contingency plans have been tested in accordance with policy
Agency/Component	Category	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed			
OARM	High	0	0	0	0	0	0	0	0	0
	Moderate	8	3	2	0	10	3	3	2	3
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	8	3	2	0	10	3	3	2	3
OCFO	High	0	0	0	0	0	0	0	0	0
	Moderate	15	2	0	0	15	2	1	2	2
	Low	1	0	0	0	1	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	16	2	0	0	16	2	1	2	2
OECA	High	0	0	0	0	0	0	0	0	0
	Moderate	7	0	0	0	7	0	0	0	0
	Low	2	1	0	0	2	1	1	1	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	9	1	0	0	9	1	1	1	0
OEI	High	0	0	0	0	0	0	0	0	0
	Moderate	17	1	4	2	21	3	3	3	3
	Low	11	2	3	0	14	2	1	1	1
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	28	3	7	2	35	5	4	4	4

Question 1: FISMA Systems Inventory & Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

		Question 1						Question 2		
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems(Agency and Contractor systems)		a. Number of systems certified and accredited	b. Number of systems for which security controls have been tested and reviewed in the past year	c. Number of systems for which contingency plans have been tested in accordance with policy
Agency/Component	Category	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed			
OGC	High	0	0	0	0	0	0	0	0	0
	Moderate	0	0	0	0	0	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	0	0	0	0	0	0	0	0	0
OIA	High	0	0	0	0	0	0	0	0	0
	Moderate	0	0	0	0	0	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	0	0	0	0	0	0	0	0	0
OIG	High	0	0	0	0	0	0	0	0	0
	Moderate	7	0	0	0	7	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	7	0	0	0	7	0	0	0	0
OPPTS	High	0	0	0	0	0	0	0	0	0
	Moderate	4	0	1	0	5	0	0	0	0
	Low	1	0	0	0	1	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	5	0	1	0	6	0	0	0	0

Question 1: FISMA Systems Inventory & Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

		Question 1						Question 2		
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems(Agency and Contractor systems)		a. Number of systems certified and accredited	b. Number of systems for which security controls have been tested and reviewed in the past year	c. Number of systems for which contingency plans have been tested in accordance with policy
Agency/Component	Category	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed			
ORD	High	0	0	0	0	0	0	0	0	0
	Moderate	5	0	0	0	5	0	0	0	0
	Low	9	1	0	0	9	1	1	1	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	14	1	0	0	14	1	1	1	0
OSWER	High	0	0	0	0	0	0	0	0	0
	Moderate	3	1	1	0	4	1	1	1	1
	Low	4	0	1	0	5	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	7	1	2	0	9	1	1	1	1
OW	High	0	0	0	0	0	0	0	0	0
	Moderate	3	1	0	0	3	1	1	0	1
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	3	1	0	0	3	1	1	0	1
R1	High	0	0	0	0	0	0	0	0	0
	Moderate	1	0	0	0	1	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	1	0	0	0	1	0	0	0	0

Question 1: FISMA Systems Inventory & Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

		Question 1						Question 2		
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems(Agency and Contractor systems)		a. Number of systems certified and accredited	b. Number of systems for which security controls have been tested and reviewed in the past year	c. Number of systems for which contingency plans have been tested in accordance with policy
Agency/Component	Category	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed			
R10	High	0	0	0	0	0	0	0	0	0
	Moderate	1	0	0	0	1	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	1	0	0	0	1	0	0	0	0
R2	High	0	0	0	0	0	0	0	0	0
	Moderate	2	0	0	0	2	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	2	0	0	0	2	0	0	0	0
R3	High	0	0	0	0	0	0	0	0	0
	Moderate	1	0	0	0	1	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	1	0	0	0	1	0	0	0	0
R4	High	0	0	0	0	0	0	0	0	0
	Moderate	1	0	0	0	1	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	1	0	0	0	1	0	0	0	0

Question 1: FISMA Systems Inventory & Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

		Question 1						Question 2		
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems(Agency and Contractor systems)		a. Number of systems certified and accredited	b. Number of systems for which security controls have been tested and reviewed in the past year	c. Number of systems for which contingency plans have been tested in accordance with policy
Agency/Component	Category	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed			
R5	High	0	0	0	0	0	0	0	0	0
	Moderate	2	1	0	0	2	1	1	1	1
	Low	1	0	0	0	1	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	3	1	0	0	3	1	1	1	1
R6	High	0	0	0	0	0	0	0	0	0
	Moderate	1	0	0	0	1	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	1	0	0	0	1	0	0	0	0
R7	High	0	0	0	0	0	0	0	0	0
	Moderate	1	0	0	0	1	0	0	0	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	1	0	0	0	1	0	0	0	0
R8	High	0	0	0	0	0	0	0	0	0
	Moderate	1	0	0	0	1	0	0	0	0
	Low	1	1	0	0	1	1	1	1	1
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	2	1	0	0	2	1	1	1	1

Question 1: FISMA Systems Inventory & Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

		Question 1						Question 2		
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems(Agency and Contractor systems)		a. Number of systems certified and accredited	b. Number of systems for which security controls have been tested and reviewed in the past year	c. Number of systems for which contingency plans have been tested in accordance with policy
Agency/Component	Category	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed			
R9	High	0	0	0	0	0	0	0	0	0
	Moderate	1	0	1	1	2	1	1	1	1
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	1	0	1	1	2	1	1	1	1
Agency Totals	High	1	0	0	0	1	0	0	0	0
	Moderate	90	10	10	3	100	13	12	11	13
	Low	35	6	5	0	40	6	5	5	3
	Not Categorized	0	0	0	0	0	0	0	0	0
	Total Systems	126	16	15	3	141	19	17	16	16

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory

The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the Agency or other organization on behalf of the Agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and Agency policy.

Agencies are responsible for ensuring the security of information systems used by a contractor of their Agency or other organization on behalf of their Agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal Agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

3a. Does the Agency have policies for oversight of contractors?

Yes

3a(1). Is the policy implemented?

Yes

Comments:	EPA's Network Security Policy states that the Agency must monitor contractor's compliance with information security responsibilities in Agency contracts. The policy is implemented; however, procedures and training could be improved for the Certification and Accreditation process.

3b. Does the Agency have a materially correct inventory of major information systems (including national security systems) operated by or under the control of such Agency?

Yes

3c. Does the Agency maintain an inventory of interfaces between the Agency systems and all other systems, such as those not operated by or under the control of the Agency?

Yes

3d. Does the Agency require agreements for interfaces between systems it owns or operates and other systems not operated by or under the control of the Agency?

Yes

3e. The Agency inventory is maintained and updated at least annually.

Yes

3f. The IG generally agrees with the CIO on the number of Agency-owned systems.

Yes

3g. The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the Agency or other organization on behalf of the Agency.

Yes

Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process

Assess whether the Agency has developed, implemented, and is managing an Agency-wide plan of action and milestones (POA&M) process, providing explanatory detail in the area provided.

4a. Has the Agency developed and documented an adequate policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts?

Yes

Comments:

EPA has developed and implemented the following:

- Procedure for Information Security Plans of Actions and Milestones (POA&Ms), dated June 18, 2004
- EPA Certification and Accreditation Process, dated May 11, 2006
- Quarterly and Annual Training to Information Security Officers on Entering POA&Ms
- Automated Process for Entering POA&Ms in Agency's tracking and reporting database

4a(1). Has the Agency fully implemented the policy?

Yes

4b. Is the Agency currently managing and operating a POA&M process?

Yes

4c. Is the Agency's POA&M process an Agency-wide process, incorporating all known IT security weakness, including IG/external audit findings associated with information systems used or operated by the Agency or by a contractor of the Agency or other organization on behalf of the Agency?

Yes

4d. Does the POA&M process prioritize IT security weakness to help ensure significant IT security weaknesses are corrected in a timely manner and receive appropriate resources?

Yes

4e. When an IT security weakness is identified, do program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)?

Yes

4f. For Systems Reviewed:

4f(1). Are deficiencies tracked and remediated in a timely manner?

Yes

4f(2). Are the remediation plans effective for correcting the security weakness?

Yes

4f(3). Are the estimated dates for remediation reasonable and adhered to?

Yes

4g. Do Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly)?

Yes

4h. Does the Agency CIO centrally track, maintain, and independently review/validate POA&M activities on at least a quarterly basis?

Yes

Question 5: IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the Agency's certification and accreditation (C&A) process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" for C&A work initiated after May 2004. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," to determine a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.

5a. Has the Agency developed and documented an adequate policy for establishing a C&A process that follows the NIST framework?

Yes

5b. Is the Agency currently managing and operating a C&A process in compliance with its policies?

Yes

5c. For Systems reviewed, does the C&A process adequately provide:

5c(1). Appropriate risk categories

Yes

5c(2). Adequate risk assessments

No

5c(3). Selection of appropriate controls

Yes

5c(4). Adequate testing of controls

No

5c(5). Regular monitoring of system risks and the adequacy of controls

Yes

5d. For systems reviewed, is the Authorizing Official presented with complete and reliable C&A information to facilitate an informed system Authorization to Operate decision based on risks and controls implemented?

No

Comments: Based on the systems selected for review, information security documentation was not complete nor accurate in order for an authorizing official to make an informed decision to authorize a system for operation.

Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process

Provide a qualitative assessment of the Agency's process, as discussed in the SAOP section, for protecting privacy-related information, including adherence to existing policy, guidance and standards. Provide explanatory information in the area provided.

6a. Has the Agency developed and documented adequate policies that comply with OMB guidance in M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information?

Yes

6b. Is the Agency currently managing and operating a privacy program with appropriate controls in compliance with its policies?

Yes

6c. Has the Agency developed and documented an adequate policy for PIAs?

Yes

6d. Has the Agency fully implemented the policy and is the Agency currently managing and operating a process for performing adequate PIAs?

Yes

Question 7: Configuration Management

7a. Is there an Agency wide security configuration policy?

Yes

7a(1). For each OS/platform/system for which your Agency has a configuration policy, please indicate the status of implementation for that policy.

OS/Platform/System	Implementation Status
Microsoft Windows 2000	**Policy fully implemented** **What tools and techniques is your Agency using for monitoring compliance?** **Tool/Technique Name** / **Tool Category** Symantec RMS, Bindview, Security Configuration Management Tool / Network Monitoring Software Lumension Patchlink / Patch Scanners

<table>
<tr><th>OS/Platform/System</th><th>Implementation Status</th></tr>
<tr><td>Redhat Enterprise Linux 4</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?
<table>
<tr><th>Tool/Technique Name</th><th>Tool Category</th></tr>
<tr><td>Unix Security Checklist, Tripwire, Enterprise Security Manager, Bindview, NOS Admin, Symantec Control Compliance Suite</td><td>Network Monitoring Software</td></tr>
</table></td></tr>
<tr><td>IBM AIX 5</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?
<table>
<tr><th>Tool/Technique Name</th><th>Tool Category</th></tr>
<tr><td>Afick, Symantec Control Compliance Suite Product</td><td>Network Monitoring Software</td></tr>
</table></td></tr>
<tr><td>Microsoft Windows XP</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?
<table>
<tr><th>Tool/Technique Name</th><th>Tool Category</th></tr>
<tr><td>Symantec RMS, Bindview,Security Configuration Management Tool</td><td>Network Monitoring Software</td></tr>
<tr><td>Lumension Patchlink</td><td>Patch Scanners</td></tr>
</table></td></tr>
<tr><td>Sun Solaris 9</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?
<table>
<tr><th>Tool/Technique Name</th><th>Tool Category</th></tr>
<tr><td>Unix Security Checklist, Tripwire, Bindview, NOS Admin Basic Security Module</td><td>Network Monitoring Software</td></tr>
<tr><td>C2 Auditing</td><td>Log Analysis Software</td></tr>
<tr><td>Enterprise Security Manager</td><td>Vulnerability Scanners</td></tr>
</table></td></tr>
</table>

OS/Platform/System	Implementation Status
Sun Solaris 10	**Policy fully implemented** **What tools and techniques is your Agency using for monitoring compliance?**

Tool/Technique Name	Tool Category
Unix Security Checklist, Tripwire, Bindview, NOS Admin Basic Security Module	Network Monitoring Software
C2 Auditing	Log Analysis Software
Enterprise Security Manager	Vulnerability Scanners

7b. Indicate the status of the implementation of Federal Desktop Core Configuration (FDCC) at your Agency:

7b(1). Agency has documented deviations from FDCC standard configuration.

Yes

7b(2). New Fedebral Acquisition Regulation 2008-004 language, which modified "Part 39-Acquisition of Information Technology," is included in all contracts related to common security settings.

Yes

8a. How often does the Agency comply with documented policies and procedures for identifying and reporting incidents internally?

90 % to 100 %

8b. How often does the Agency comply with documented policies and procedures for timely reporting of incidents to US-CERT?

90 % to 100 %

8c. How often does the Agency follow documented policies and procedures for reporting to law enforcement?

90 % to 100 %

Question 9: Security Awareness Training

Provide an assessment of whether the Agency has provided IT security awareness training to all users with log-in privileges, including contractors. Also provide an assessment of whether the Agency has provided appropriate training to employees with significant IT security responsibilities.

9a. Has the Agency developed and documented an adequate policy for identifying all general users, contractors, and system owners/employees who have log-in privileges, and providing them with suitable IT security awareness training?

Yes

9b. Report the following for your Agency:

9b(1). Total number of people with log-in privileges to Agency systems.

22,325

9b(2). Number of people with log-in privileges to Agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program."

22,281 (100 %)

9b(3). Total number of employees with significant information security responsibilities.

507

9b(4). Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model."

491 (97 %)

Question 10: Peer-to-Peer File Sharing

10. Does the Agency explain policies regarding the use of peer-to-peer file sharing in IT security awareness training, ethics training, or any other Agency-wide training?

Yes

Appendix A

Summary of Significant Fiscal Year 2009 Security Control Audits

During Fiscal Year 2009, the U.S. Environmental Protection Agency's (EPA's) Office of Inspector General (OIG) initiated the following audits of EPA's information technology security program and information systems. The following synopsizes key findings.

1. Improved Security Planning Needed for the Customer Technology Solutions (CTS) Project, Report No. 10-P-0028, November 16, 2009

In general, EPA needs to (1) direct the CTS contractor to develop and implement a vulnerability testing and remediation process for CTS equipment, (2) issue a memorandum to Agency Senior Information Officials requiring their program office to conduct vulnerability testing of CTS equipment until a formal vulnerability testing and management process with CTS has been established, (3) require the CTS contractor to remediate identified vulnerabilities in a timely manner and inform the respective Senior Information Official when they complete the corrective action, and (4) ensure all key actions outlined in the conditional CTS authorization to operate are completed by the defined milestone dates.

2. Project Delays Prevent EPA from Implementing an Agency-wide Information Security Vulnerability Management Program, Report No. 09-P-0240, September 21, 2009

EPA needs to (1) create plans of action and milestones for unimplemented recommendations, (2) update the Management Audit Tracking System to show the status of each implemented audit recommendation, (3) provide EPA program and regional offices with an alternative solution for vulnerability management, (4) establish a workgroup to solicit input on training needs and facilitate rolling out the Agency-wide vulnerability management program, and (5) issue an updated memorandum discussing guidance and requirements.

EPA concurred with the recommendations and subsequently implemented corrective actions to adequately address the report recommendations.

3. ECHO Data Quality Audit – Phase I Results: The Integrated Compliance Information System Needs Security Controls to Protect Significant Non-Compliance Data, Report No. 09-P-0226, August 31, 2009

EPA needs to implement data security features to limit the end users' ability to change data field information. EPA plans to explore additional options to restrict manual override of data field information.

4. EPA Should Delay Deploying Its New Acquisition System until Testing Is Completed, Report No. 09-P-0197, July 20, 2009

EPA needs to (1) identify and document all system requirements; (2) update, review, and implement formal testing policies and procedures; (3) test all system requirements; (4) update the project schedule to communicate the current status of and future project activities; and (5) develop and implement oversight procedures to ensure system development activities and future projects adhere to all requirements.

EPA concurred with the findings and will delay deployment until the next fiscal year.

5. Steps Taken But More Work Needed to Strengthen Governance, Increase Utilization, and Improve Security Planning for the Exchange Network, Report No. 09-P-0184, June 30, 2009

In general, EPA needs to (1) submit an updated correction action plan for unimplemented recommendations, (2) recertify and reaccredit the Central Data Exchange, (3) update the Central Data Exchange security plan and develop the contingency plan in accordance with federal guidance, and (4) conduct a formal, independent risk assessment for the Central Data Exchange.

6. Lack of Project Plan Resulted in Transition and Contractor Performance Problems for the Institutional Controls Tracking System, Report No. 09-P-0128, March 25, 2009

In general, EPA needs to (1) document procedures for overseeing development activities as prescribed by Agency guidance, and (2) conduct and document a review of system documentation to ensure the document is current.

EPA concurred with findings and recommendations and provided a complete corrective action plan to address the report's recommendations.

7. Review of the Quality of Self-Reported Security Information in EPA's Automated Security Self-Evaluation and Remediation Tracking (ASSERT) System, Assignment No. 2008-0003

The primary objective of this assignment is to determine whether EPA has implemented effective management control processes for maintaining the quality of the data in EPA's ASSERT system. The OIG plans to issue a final report by December 2009.

As part of the Fiscal Year 2009 Federal Information Security Management Act audit, the following series of network vulnerability reports were issued to EPA's offices to address high-risk vulnerabilities:

- Results of Technical Network Vulnerability Assessment: EPA's Great Lakes National Program Office, Report No. 09-P-0185, June 30, 2009
- Results of Technical Network Vulnerability Assessment: EPA's National Computer Center, Report No. 09-P-0186, June 30, 2009
- Results of Technical Network Vulnerability Assessment: Region 8, Report No. 09-P-0187, June 30, 2009
- Results of Technical Network Vulnerability Assessment: EPA's Potomac Yard Buildings, Report No. 09-P-0188, June 30, 2009
- Results of Technical Network Vulnerability Assessment: EPA's 1310 L Street Building, Report No. 09-P-0189, June 30, 2009
- Results of Technical Network Vulnerability Assessment: EPA's Research Triangle Park Finance Center, Report No. 09-P-0227, August 31, 2009

EPA officials developed plans of action and milestones to remediate the network vulnerabilities.

As part of the Fiscal Year 2008 Federal Information Security Management Act audit, the following series of network vulnerability reports were issued to EPA's offices to address high- and medium-risk vulnerabilities:

- Results of Technical Network Vulnerability Assessment: EPA Headquarters, Report No. 09-P-0097, February 23, 2009
- Results of Technical Network Vulnerability Assessment: EPA's Research Triangle Park Campus, Report No. 09-P-0055, December 9, 2008
- Results of Technical Network Vulnerability Assessment: EPA's Las Vegas Finance Center, Report No. 09-P-0054, December 9, 2008
- Results of Technical Network Vulnerability Assessment: EPA's Radiation and Indoor Environments National Laboratory, Report No. 09-P-0053, December 9, 2008
- Results of Technical Network Vulnerability Assessment: Region 9, Report No. 09-P-0052, December 9, 2008

EPA officials developed plans of action and milestones to remediate the network vulnerabilities.

Appendix B

Distribution

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