U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Fiscal Year 2012 Federal Information Security Management Act Report

Status of EPA’s Computer Security Program

Report No. 13-P-0032 **October 26, 2012**

Report Contributors:

Rudolph M. Brevard
Cheryl Reid
Vincent Campbell
Albert Schmidt
Nii-Lantei Lamptey
Rodney Allison
Kyle Denning

Abbreviations

AC	Access Control
ASSERT	Automated System Security Evaluation and Remediation Tracking
BIA	Business Impact Analysis
CA	Security Assessment and Authorization
CIO	Chief Information Officer
CPIC	Capital Planning and Investment Control
DSS	Directory Service System
EPA	U.S. Environmental Protection Agency
FCD	Federal Continuity Directive
FDCC	Federal Desktop Core Configurations
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	U.S. Government Accountability Office
HSPD	Homeland Security Presidential Directive
IFMS	Integrated Financial Management System
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OEI	Office of Environmental Information
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identification Verification
PM	Program Management
POA&M	Plan of Action & Milestones
SA	System and Services Acquisitions
SIEM	Security Incident and Event Management
SP	Special Publication
TT&E	Test, Training, and Exercise
USGCB	United States Government Configuration Baseline
US-CERT	United States Computer Emergency Readiness Team

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

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

THE INSPECTOR GENERAL

October 26, 2012

MEMORANDUM

SUBJECT: Fiscal Year 2012 Federal Information Security Management Act Report:
Status of EPA’s Computer Security Program
Report No. 13-P-0032

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

TO: Lisa P. Jackson
Administrator

Attached is the Office of Inspector General’s (OIG’s) Fiscal Year 2012 Federal Information Security Management Act (FISMA) Reporting Template, as prescribed by the Office of Management and Budget (OMB). We performed this review in accordance with generally accepted government auditing standards. These standards require the team to plan and perform the review to obtain sufficient and appropriate evidence to provide a reasonable basis for the findings and conclusions based on the objectives of the review.

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 of OMB.

The audit work performed during the FISMA review disclosed that the Agency needs to make improvements in the following programs: (1) Continuous Monitoring Management, (2) Configuration Management, and (3) Risk Management. The Agency concurred with our findings.

In addition, audit work during fiscal year 2012 noted significant weaknesses with several aspects of EPA’s information security program. Appendix A summarizes the results from these audit reports.

Inspector General

Section Report

2012

Annual FISMA Report

Environmental Protection Agency

Section 1: Continuous Monitoring Management

1.1 **Has the Organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:**

No

1.1.1 **Documented policies and procedures for continuous monitoring (NIST 800-53: CA-7)**

Yes

1.1.2 **Documented strategy and plans for continuous monitoring (NIST 800-37 Rev 1, Appendix G)**

No

Comments: The Agency finalized a Continuous Monitoring (CM) Strategy in June 2012. However, the Agency has not yet fully implemented a plan for CM.

1.1.3 **Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST 800-53, NIST 800-53A)**

No

Comments: The Agency performs assessments of system security controls. However, the Agency is working towards implementing a continuous monitoring plan that includes ongoing assessments of security controls.

1.1.4 **Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions and updates with the frequency defined in the strategy and/or plans (NIST 800-53, NIST 800-53A)**

Yes

1.2 **Please provide any additional information on the effectiveness of the Organization’s Continuous Monitoring Management Program that was not noted in the questions above**

The OIG has issued several reports from Fiscal Years 2011 and 2012 identifying continued weaknesses in the Agency's continuous monitoring program.

Comments: Recently, the OIG reported that the Agency is not conducting follow-up with system owners to confirm that identified vulnerabilities have been addressed or request that system owners provide a response or evidence that the vulnerabilities have been addressed.

Section 2: Configuration Management

Section 2: Configuration Management

2.1 **Has the Organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:**

No

2.1.1 **Documented policies and procedures for configuration management**

Yes

2.1.2 **Standard baseline configurations defined**

Yes

2.1.3 **Assessing for compliance with baseline configurations**

No

2.1.4 **Process for timely, as specified in Organization policy or standards, remediation of scan result deviations**

No

2.1.5 **For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented**

No

2.1.6 **Documented proposed or actual changes to hardware and software configurations**

Yes

2.1.7 **Process for timely and secure installation of software patches**

No

2.1.8 **Software assessing (scanning) capabilities are fully implemented (NIST 800-53: RA-5, SI-2)**

No

2.1.9 **Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in Organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)**

No

2.1.10 **Patch management process is fully developed, as specified in Organization policy or standards. (NIST 800-53: CM-3, SI-2)**

No

Section 2: Configuration Management

2.2 **Please provide any additional information on the effectiveness of the Organization’s Configuration Management Program that was not noted in the questions above.**

In July 2012, the Government Accountability Office (GAO) issued report "INFORMATION SECURITY: Environmental Protection Agency Needs to Resolve Weaknesses," Report No. GAO-12-696.

Comments: GAO reported that EPA had not always implemented configuration management controls. Although the Agency has an automated tool in place for managing changes, officials could only provide records of approved changes for four of the six systems reviewed. Information for the other two systems consisted only of e-mails describing the changes. Change information provided by the system owners varied in content, and the Agency-wide configuration management guide did not instruct them on how such records should be documented. Further, EPA had not securely configured its networks and databases in accordance with NIST guidance and Web applications, and operating systems were not always configured to the most restrictive settings in accordance with NIST guidance. Some EPA information systems and network devices were running outdated software that was no longer supported by the manufacturer, resulting in EPA being unable to effectively patch them for vulnerabilities.

Section 3: Identity and Access Management

3.1 **Has the Organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes:**

Yes

3.1.1 **Documented policies and procedures for account and identity management (NIST 800-53: AC-1)**

Yes

3.1.2 **Identifies all users, including federal employees, contractors, and others who access Organization systems (NIST 800-53, AC-2)**

No

3.1.3 **Identifies when special access requirements (e.g., multi-factor authentication) are necessary.**

Yes

3.1.4 **If multi-factor authentication is in use, it is linked to the Organization's PIV program where appropriate (NIST 800-53, IA-2)**

Yes

Section 3: Identity and Access Management

3.1.5 **Organization has adequately planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11)**

Yes

3.1.6 **Ensures that the users are granted access based on needs and separation of duties principles**

Yes

3.1.7 **Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users (For example: IP phones, faxes, printers are examples of devices attached to the network that are distinguishable from desktops, laptops or servers that have user accounts)**

Yes

3.1.8 **Identifies all User and Non-User Accounts (refers to user accounts that are on a system. Examples of non-user accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users)**

Yes

3.1.9 **Ensures that accounts are terminated or deactivated once access is no longer required**

No

3.1.10 **Identifies and controls use of shared accounts**

No

3.2 **Please provide any additional information on the effectiveness of the Organization’s Identity and Access Management Program that was not noted in the questions above.**

In July 2012, GAO issued report "INFORMATION SECURITY: Environmental Protection Agency Needs to Resolve Weaknesses," Report No. GAO-12-696.

Comments:

GAO reported that (1) EPA did not always protect network boundaries, (2) EPA users were not always properly identified and authenticated, (3) authorization controls were not fully implemented, and (4) EPA did not always implement physical controls. The OIG also issued a report in September 2012, "EPA Should Improve Management Practices and Security Controls for Its Network Directory Service System and Related Servers," Report No. 12-P-0836. OIG reported EPA is not managing key system documentation, system administration functions, and the granting and monitoring of privileged accounts of its directory service system (DSS). EPA is not performing DSS user account administration practices, and does not have a management oversight process to ensure that the regions and program offices are managing their delegated responsibilities in accordance with Agency and federal requirements.

Section 4: Incident Response and Reporting

4.1 Has the Organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

4.1.1 Documented policies and procedures for detecting, responding to and reporting incidents (NIST 800-53: IR-1)

Yes

4.1.2 Comprehensive analysis, validation and documentation of incidents

Yes

4.1.3 When applicable, reports to US-CERT within established timeframes (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)

Yes

4.1.4 When applicable, reports to law enforcement within established timeframes (SP 800-86)

No

4.1.5 Responds to and resolves incidents in a timely manner, as specified in Organization policy or standards, to minimize further damage. (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)

Yes

4.1.6 Is capable of tracking and managing risks in a virtual/cloud environment, if applicable

Yes

4.1.7 Is capable of correlating incidents

Yes

4.1.8 There is sufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)

Yes

4.2 Please provide any additional information on the effectiveness of the Organization’s Incident Management Program that was not noted in the questions above.

No additional information reported.

Section 5: Risk Management

Section 5: Risk Management

5.1 **Has the Organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:**

No

5.1.1 **Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process**

Yes

5.1.2 **Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev.1**

No

5.1.3 **Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev.1**

No

5.1.4 **Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1**

No

5.1.5 **Categorizes information systems in accordance with government policies**

Yes

5.1.6 **Selects an appropriately tailored set of baseline security controls**

Yes

5.1.7 **Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation**

Yes

5.1.8 **Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system**

Yes

Section 5: Risk Management

5.1.9 **Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable**

Yes

5.1.10 **Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials**

Yes

5.1.11 **Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization.**

No

5.1.12 **Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO).**

No

5.1.13 **Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks**

Yes

5.1.14 **Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies. (SP 800-18, SP 800-37)**

Yes

5.1.15 **Security authorization package contains Accreditation boundaries for Organization information systems defined in accordance with government policies.**

Yes

5.2 **Please provide any additional information on the effectiveness of the Organization's Risk Management Program that was not noted in the questions above.**

In July 2012, GAO issued report "INFORMATION SECURITY: Environmental Protection Agency Needs to Resolve Weaknesses," Report No. GAO-12-696.

Comments: GAO reported that EPA did not (1) always effectively encrypt sensitive information, (2) effectively log and monitor system activity, (3) always implement media protection controls, and (4) document that system security controls were fully tested. GAO also found that System Security Plans referenced outdated policies and procedures.

Section 6: Security Training

6.1 **Has the Organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:**

Yes

6.1.1 **Documented policies and procedures for security awareness training (NIST 800-53: AT-1)**

Yes

6.1.2 **Documented policies and procedures for specialized training for users with significant information security responsibilities**

Yes

6.1.3 **Security training content based on the organization and roles, as specified in Organization policy or standards**

Yes

6.1.4 **Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other Organization users) with access privileges that require security awareness training**

Yes

6.1.5 **Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other Organization users) with significant information security responsibilities that require specialized training**

Yes

6.1.6 **Training material for security awareness training contains appropriate content for the Organization (SP 800-50, SP 800-53).**

Yes

6.2 **Please provide any additional information on the effectiveness of the Organization’s Security Training Program that was not noted in the questions above.**

In July 2012, GAO issued report "INFORMATION SECURITY: Environmental Protection Agency Needs to Resolve Weaknesses," Report No. GAO-12-696.

Comments:	GAO reported that the Agency needs to develop and finalize a role-based security training procedure that tailors specific training requirements to EPA users' role/position descriptions and details the actions information security officers must take when users do not complete the training.

Section 7: Plan Of Action & Milestones (POA&M)

Section 7: Plan Of Action & Milestones (POA&M)

7.1 **Has the Organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:**

Yes

7.1.1 **Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation**

Yes

7.1.2 **Tracks, prioritizes and remediates weaknesses**

Yes

7.1.3 **Ensures remediation plans are effective for correcting weaknesses**

No

7.1.4 **Establishes and adheres to milestone remediation dates**

Yes

7.1.5 **Ensures resources are provided for correcting weaknesses**

Yes

7.1.6 **POA&Ms include security weaknesses discovered during assessments of security controls and requiring remediation. (Do not need to include security weakness due to a Risk Based Decision to not implement a security control) (OMB M-04-25)**

No

7.1.7 **Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25)**

Yes

7.1.8 **Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25)**

Yes

Section 7: Plan Of Action & Milestones (POA&M)

7.2 **Please provide any additional information on the effectiveness of the Organization's POA&M Program that was not noted in the questions above.**

In July 2012, GAO issued report "INFORMATION SECURITY: Environmental Protection Agency Needs to Resolve Weaknesses," Report No. GAO-12-696.

Comments: GAO reported that (1) the manner in which the EPA uses the Automated System Security Evaluation and Remediation Tracking (ASSERT) tool for POA&Ms can preclude retrieval of specific POA&Ms and pose weaknesses with data reliability because entries lacked a specific description of each weakness and did not list the report where the weakness had initially been identified, and (2) ASSERT does not have built-in safeguards to keep individuals who have access to POA&Ms from altering initial milestone and completion dates.

Section 8: Remote Access Management

8.1 **Has the Organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:**

Yes

8.1.1 **Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST 800-53: AC-1, AC-17)**

Yes

8.1.2 **Protects against unauthorized connections or subversion of authorized connections.**

Yes

8.1.3 **Users are uniquely identified and authenticated for all access (NIST 800-46, Section 4.2, Section 5.1)**

Yes

8.1.4 **Telecommuting policy is fully developed (NIST 800-46, Section 5.1)**

Yes

8.1.5 **If applicable, multi-factor authentication is required for remote access (NIST 800-46, Section 2.2, Section 3.3)**

Yes

Section 8: Remote Access Management

8.1.6 **Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms**

Yes

8.1.7 **Defines and implements encryption requirements for information transmitted across public networks**

Yes

8.1.8 **Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication are required**

Yes

8.1.9 **Lost or stolen devices are disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines)**

Yes

8.1.10 **Remote access rules of behavior are adequate in accordance with government policies (NIST 800-53, PL-4)**

Yes

8.1.11 **Remote access user agreements are adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6)**

Yes

8.2 **Please provide any additional information on the effectiveness of the Organization’s Remote Access Management that was not noted in the questions above.**

No additional information reported.

Section 9: Contingency Planning

9.1 **Has the Organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:**

Yes

9.1.1 **Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST 800-53: CP-1)**

Yes

Section 9: Contingency Planning

9.1.2 **The Organization has performed an overall Business Impact Analysis (BIA) (NIST SP 800-34)**

No

9.1.3 **Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures (NIST SP 800-34)**

Yes

9.1.4 **Testing of system specific contingency plans**

Yes

9.1.5 **The documented business continuity and disaster recovery plans are in place and can be implemented when necessary (FCD1, NIST SP 800-34)**

Yes

9.1.6 **Development and fully implementable of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST 800-53)**

Yes

9.1.7 **Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans**

Yes

9.1.8 **After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34)**

Yes

9.1.9 **Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53)**

Yes

9.1.10 **Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53)**

No

9.1.11 **Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53)**

Yes

9.1.12 **Contingency planning that consider supply chain threats**

No

Section 9: Contingency Planning

9.2 Please provide any additional information on the effectiveness of the Organization’s Contingency Planning Program that was not noted in the questions above.

In July 2012, GAO issued report "INFORMATION SECURITY: Environmental Protection Agency Needs to Resolve Weaknesses," Report No. GAO-12-696.

Comments: GAO reported that (1) the Agency did not follow its own procedures or NIST guidance for approving contingency plans, reviewing them annually, and updating them as necessary; (2) EPA did not provide clear evidence that contingency plans were included in certification and authorization packages or evidence of having had an annual review; and (3) among the six plans reviewed, five did not provide full contact information for some staff listed, giving only office telephone numbers and e-mail addresses or, in some cases, office numbers alone.

Section 10: Contractor Systems

10.1 Has the Organization established a program to oversee systems operated on its behalf by contractors or other entities, including Organization systems and services residing in the cloud external to the Organization? Besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes:

Yes

10.1.1 Documented policies and procedures for information security oversight of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud

Yes

10.1.2 The Organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and Organization guidelines

Yes

10.1.3 A complete inventory of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud

Yes

10.1.4 The inventory identifies interfaces between these systems and Organization-operated systems (NIST 800-53: PM-5)

Yes

Section 10: Contractor Systems

10.1.5 **The Organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates**

Yes

10.1.6 **The inventory of contractor systems is updated at least annually.**

Yes

10.1.7 **Systems that are owned or operated by contractors or entities, including Organization systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines**

Yes

10.2 **Please provide any additional information on the effectiveness of the Organization's Contractor Systems Program that was not noted in the questions above.**

In July 2012, GAO issued report "INFORMATION SECURITY: Environmental Protection Agency Needs to Resolve Weaknesses," Report No. GAO-12-696.

Comments: GAO reported that the Agency did not properly ensure that its inventory of information systems, including those systems operated by contractors, was accurate.

Section 11: Security Capital Planning

11.1 **Has the Organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:**

Yes

11.1.1 **Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process**

Yes

11.1.2 **Includes information security requirements as part of the capital planning and investment process**

Yes

11.1.3 **Establishes a discrete line item for information security in organizational programming and documentation (NIST 800-53: SA-2)**

Yes

11.1.4 **Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST 800-53: PM-3)**

Yes

Section 11: Security Capital Planning

11.1.5 Ensures that information security resources are available for expenditure as planned

Yes

11.2 Please provide any additional information on the effectiveness of the Organization's Security Capital Planning Program that was not noted in the questions above.

No additional information reported.

Appendix A

Summary of Significant Fiscal Year 2012 Security Control Audits

During fiscal year 2012, the EPA OIG published a number of audit reports on EPA's information technology security program and information systems. The following summarizes key findings:

1. ***Improvements Needed in EPA's Network Security Monitoring Program*, Report No. 12-P-0899, September 27, 2012.**

   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. 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 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. The Agency concurred with our recommendations.

2. ***EPA's Office of Environmental Information Should Improve Ariel Rios and Potomac Yard Computer Room Security Controls*, Report No. 12-P-0879, September 26, 2012.**

   The security posture and in-place environmental control review of the computer rooms in the Ariel Rios and Potomac Yard buildings revealed numerous security and environmental control deficiencies. These control deficiencies greatly reduce the ability of the Office of Environmental Information (OEI) to safeguard critical information technology assets and associated data from the risk of damage and/or loss. The Agency agreed with two recommendations and disagreed with three other recommendations. OEI disagreed because it asserts that the Office of Administration and Resources Management bears responsibility for remediation for two of the recommendations, and for the other recommendation it stated that it is already monitoring environmental variable information. During the audit, the OIG requested policies and procedures that address limiting water damage to IT assets. OEI did not provide any documentation in response to this request and the OIG concluded that such policies did not exist. The OIG believes that OEI bears the responsibility for addressing these recommendations because OEI is responsible for managing IT assets in the Ariel Rios and Potomac Yard computer rooms.

3. ***EPA's Radiation and Indoor Environments National Laboratory Should Improve Its Computer Room Security Controls*, Report No. 12-P-0847, September 21, 2012.**

   Our review of the security posture and in-place environmental controls of EPA's Radiation and Indoor Environments National Laboratory computer room disclosed an array of security and environmental control deficiencies. These deficiencies greatly hinder the ability of the Office of Air and Radiation to safeguard critical information technology assets and associated data from the risk of damage and/or loss. The Agency concurred with our recommendations.

4. ***EPA Should Improve Management Practices and Security Controls for Its Network Directory Service System and Related Servers,* Report No. 12-P-0836, September 20, 2012.**

   OEI is not managing key system management documentation, system administration functions, the granting and monitoring of privileged accounts, and the application of environmental and physical security controls associated with its directory service system (DSS). OEI is not keeping management documentation associated with the DSS current and complete, and does not have an effective process for maintaining this documentation. Further, OEI is not performing user account administration practices for the DSS, and does not have a management oversight process to ensure that the regions and program offices are managing their delegated responsibilities in accordance with Agency and federal requirements. The Office of Administration and Resources Management's Human Resources and Contractor Management systems and processes are not linked to the user account management function. OEI is also not managing the delegation of DSS logging and monitoring processes.
   OEI and the Office of Administration and Resources Management concurred with all recommendations, other than two associated with environmental and physical security controls, and completed or agreed to take corrective actions to address the recommendations with which they concurred. OEI indicated that the particular physical and environmental controls are not its responsibility. We disagree. The DSS Authentication and Authorization servers belong to OEI, which is responsible for managing this equipment. Therefore, OEI needs to ensure that these controls are in place.

5. ***EPA Did Not Properly Migrate General Ledger Balances to Compass From the Integrated Financial Management System,* Report No. 12-P-0559, July 9, 2012.**

   EPA did not properly migrate general ledger balances to Compass from the Integrated Financial Management System. We found differences in certain fiscal year 2012 beginning balances, abnormal balances, and Agency adjustments to beginning balances. The Federal Managers' Financial Integrity Act requires agencies to provide reasonable assurance that accounts are properly recorded and accounted for to ensure reliability of financial reporting. The errors we found are indicators of internal control and oversight weaknesses in the migration of balances. The Agency stated it has taken corrective actions and will provide supporting documentation.

6. ***EPA Data Standards Plan Completed but Additional Steps Are Needed*, Report No. 12-P-0519, June 5, 2012.**

   Although EPA completed the steps listed in its corrective action plan to close out the Agency-level weakness on data standards, the actions taken were either incomplete or lacked steps to help management determine the overall effectiveness of the Agency's implementation of data standards. In particular, we determined that EPA developed a data standards training program. However, management took no steps to identify who needed the training, track whether the appropriate personnel took the training, or obtain feedback from staff on the training to ascertain the training's effectiveness. Further, we determined that EPA created data standards report cards. However, these report cards are inaccurate because EPA offices did not update the system used to create the report cards. Also, the report card format is such that management could not clearly see whether individual offices were in compliance with data standards. Also, we determined that EPA completed two conformance reviews to determine system compliance with the data standards. However, management made no plans to conduct additional reviews. The Agency agreed with the recommendations.

7. ***Office of Environmental Information Should Strengthen Controls Over Mobile Devices*, Report No. 12-P-0427, April 25, 2012.**

   OEI has no organization-wide standard operating procedures that explain responsibilities for OEI employees and contractors regarding mobile devices. OEI currently does not have effective controls for the five areas of concern noted in the hotline complaint: issuance, disconnection, multiple devices, inappropriate use, and tracking and recovery. OEI has also not established controls to determine when to disconnect devices; over a 6-month period in 2011, 68 OEI employees had zero usage of their mobile devices but incurred costs of about $29,360. Finally, procedures and controls for tracking and recovering mobile devices are missing or ineffective. OEI concurred with the majority of our recommendations and described planned actions to address our recommendations. Our recommendations remain open pending OEI's corrective action plan with milestone dates, as well as additional specificity from OEI on monitoring inappropriate device usage.

8. **Technical Vulnerability Assessments**

   As part of the fiscal year 2012 FISMA audit, the OIG issued a series of network vulnerability reports to EPA offices to address high-risk and medium-risk vulnerabilities. The OIG met with EPA information security personnel to discuss the findings. If not resolved, these vulnerabilities could expose EPA's assets to unauthorized access and potentially harm the Agency's network.

   - *Results of Technical Network Vulnerability Assessment: EPA's National Vehicle and Fuel Emissions Laboratory*, Report No. 12-P-0900, September 27, 2012.
   - Results *of Technical Network Vulnerability Assessment: EPA's Region 6*, Report No. 12-P-0659, August 10, 2012.
   - *Results of Technical Network Vulnerability Assessment: EPA's Region 1,* Report No. 12-P-0518, June 5, 2012.
   - *Region 10 Technical and Computer Room Security Vulnerabilities Increase Risk to EPA's Network*, Report No. 12-P-0220, January 20, 2012.

Appendix B

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information and Chief Information Officer
Deputy Assistant Administrator for Environmental Information
Director, Office of Technology Operations and Planning, Office of Environmental Information
Senior Agency Information Security Officer, 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 Information
Audit Follow-Up Coordinator, Office of Environmental Information