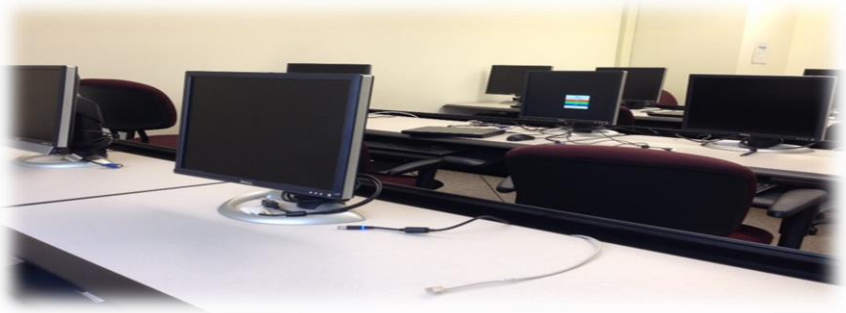
U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Information Technology

Fiscal Year 2014 Federal Information Security Management Act Report: Status of EPA's Computer Security Program

Report No. 15-P-0020 **November 13, 2014**



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

Report Contributors:

Rudolph M. Brevard
Charles M. Dade
Albert E. Schmidt
Neven Soliman
Nii-Lantei Lamptey

Abbreviations

BCP	Business Continuity Plan
BIA	Business Impact Analysis
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COOP	Continuity of Operations Plan
DRP	Disaster Recovery Plan
EPA	U.S. Environmental Protection Agency
FCD1	Federal Continuity Directive 1
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	U.S. Government Accountability Office
HSPD	Homeland Security Presidential Directive
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action & Milestones
SP	Special Publication
US-CERT	U.S. Computer Emergency Readiness Team
USGCB	U.S. Government Configuration Baseline

Cover photo: Computers on the EPA's network. (EPA OIG photo)

Are you aware of fraud, waste or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, DC 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG_Hotline@epa.gov

More information at www.epa.gov/oig/hotline.html.

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, DC 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates
Follow us on Twitter @EPAoig
Send us your Project Suggestions

U.S. Environmental Protection Agency
Office of Inspector General

15-P-0020
November 13, 2014

At a Glance

Why We Did This Review

The Office of the Inspector General conducted this review to assess the U.S. Environmental Protection Agency's (EPA's) compliance with the Federal Information Security Management Act (FISMA). FISMA requires Inspectors General to prepare an annual evaluation of their agencies' information security programs and practices. The Department of Homeland Security issued reporting guidelines requesting information on 11 information system security practices within federal agencies.

This report addresses the following EPA goal or cross-agency strategy:

- *Embracing EPA as a high-performing organization.*

Send all inquiries to our public affairs office at (202) 566-2391 or visit www.epa.gov/oig.

The full report is at:
www.epa.gov/oig/reports/2014/20141113-15-P-0020.pdf

Fiscal Year 2014 Federal Information Security Management Act Report: Status of EPA's Computer Security Program

What We Found

The EPA has established an agencywide information security program for assessing the security state of information systems that is consistent with FISMA requirements and applicable policy and guidelines for the following areas:

- Continuous Monitoring.
- Identity and Access Management.
- Incident Response and Reporting.
- Risk Management.
- Security Training.
- Plan of Action and Milestones.
- Remote Access Management.
- Contingency Planning.
- Contractor Systems.
- Security Capital Planning.

The lack of a fully developed Configuration Management program places the EPA's network at a greater risk of being compromised.

However, the EPA should place more emphasis on remediating deficiencies found within the agency's Configuration Management program. Specifically, the agency should take steps to:

- Address deviations identified by scans in a timely manner.
- Maintain documentation of baseline scans of servers and network appliances.
- Install patches in a secure and timely manner.

Additionally, in conducting the review of the Contingency Planning section of FISMA, we found that the EPA currently has an outdated Business Impact Analysis.

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

THE INSPECTOR GENERAL

November 13, 2014

MEMORANDUM

SUBJECT: Fiscal Year 2014 Federal Information Security Management Act Report: Status of EPA's Computer Security Program
Report No. 15-P-0020

FROM: Arthur A. Elkins Jr.

TO: Gina McCarthy, Administrator

This is our final report on the subject Fiscal Year 2014 Federal Information Security Management Act (FISMA) Reporting Template prepared by the Office of Inspector General of the U.S. Environmental Protection Agency (EPA). We performed this audit in accordance with generally accepted government auditing standards. Those standards require the team to plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for the findings and conclusions based on the objectives of the audit. 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 the Office of Management and Budget (OMB). In accordance with OMB reporting instructions, we are forwarding this report to you for submission, along with the agency's required information, to the Director of OMB.

We briefed agency officials on the results of our audit work and, where appropriate, made adjustments in the Continuous Monitoring Section based on additional information provided by the EPA Office of Environmental Information. The agency needs to make improvements in its Configuration Management program.

The office responsible for the issues evaluated in this report is the Office of Environmental Information's Office of Technology Operations and Planning.

We will post this report to our website at http://www.epa.gov/oig.

Inspector General

Section Report

2014

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?**

Yes

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

Yes

1.1.2 **Documented strategy for information security continuous monitoring (ISCM).**

Yes

1.1.3 **Implemented ISCM for information technology assets.**

No

1.1.4 **Evaluate risk assessments used to develop their ISCM strategy.**

Yes

1.1.5 **Conduct and report on ISCM results in accordance with their ISCM strategy.**

Yes

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

Yes

1.1.7 **Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 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.**

N/A

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 **Defined standard baseline configurations.**

Yes

2.1.3 **Assessments of 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, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented.**

Yes

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 SP 800-53: RA-5, SI-2).**

Yes

2.1.9 **Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards. (NIST SP 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 SP 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.

N/A

2.3 Does the organization have an enterprise deviation handling process and is it integrated with the automated capability.

No

2.3.1 Is there a process for mitigating the risk introduced by those deviations?

No

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 SP 800-53: AC-1).

Yes

3.1.2 Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2).

Yes

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 SP 800-53, IA-2).

Yes

3.1.5 Organization has 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 Organization has adequately planned for implementation of PIV for physical 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

Section 3: Identity and Access Management

3.1.7 Ensures that the users are granted access based on needs and separation-of-duties principles.

Yes

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

Yes

3.1.9 Identifies all user and non-user accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.)

Yes

3.1.10 Ensures that accounts are terminated or deactivated once access is no longer required.

No

3.1.11 Identifies and controls use of shared accounts.

Yes

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.

N/A

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 SP 800-53: IR-1).

Yes

4.1.2 Comprehensive analysis, validation and documentation of incidents.

Yes

Section 4: Incident Response and Reporting

4.1.3 When applicable, reports to US-CERT within established timeframes (NIST SP 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 (NIST SP 800-61).

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 SP 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.

No

4.1.7 Is capable of correlating incidents.

Yes

4.1.8 Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; 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.

N/A

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?

Yes

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

Yes

Section 5: Risk Management

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 SP 800-37, Rev.1.

Yes

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

Yes

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

Yes

5.1.5 Has an up-to-date system inventory.

No

5.1.6 Categorizes information systems in accordance with government policies.

Yes

5.1.7 Selects an appropriately tailored set of baseline security controls.

Yes

5.1.8 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

5.1.9 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

5.1.10 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

Section 5: Risk Management

5.1.11 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

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

Yes

5.1.13 Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).

Yes

5.1.14 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

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

Yes

5.1.16 Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems.

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.

N/A

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

Section 6: Security Training

6.1.1 Documented policies and procedures for security awareness training (NIST SP 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.

No

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 (NIST SP 800-50,800-53).

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.

The OIG issued "EPA's Information Systems and Data Are at Risk Due to Insufficient Training of Personnel With Significant Information Security Responsibilities," Report No. 14-P-0142, dated March 21, 2014, which documented that the "EPA lacks an information security role-based training program that defines specific training requirements for personnel with significant information security responsibilities. Implementation of the EPA's information security training program is hindered by inconsistent assignment of information security roles across the various EPA offices. The current training program does not consider specific needs of technical and managerial personnel responsibilities for implementing information security as required by the federal guidance."

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

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

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

Yes

7.1.2 **Tracks, prioritizes, and remediates weaknesses.**

Yes

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

Yes

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

Yes

7.1.5 **Ensures resources and ownership are provided for correcting weaknesses.**

No

7.1.6 **POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25).**

Yes

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

No

7.1.8 **Program officials 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; OMB M-04-25).**

Yes

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.**

N/A

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 SP 800-46, Section 4.2, Section 5.1).

Yes

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

Yes

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

Yes

8.1.6 Authentication mechanisms meet NIST SP 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 with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.

Yes

8.1.9 Lost or stolen devices are disabled and appropriately reported (NIST SP 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 SP 800-53, PL-4).

Yes

Section 8: Remote Access Management

8.1.11 Remote access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1, NIST SP 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.

N/A

8.3 Does the organization have a policy to detect and remove unauthorized (rogue) connections?

Yes

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 SP 800-53: CP-1).

Yes

9.1.2 The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (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 BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).

No

Section 9: Contingency Planning

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

Yes

9.1.7 Testing or exercising of BCP and DRP 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 not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

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 considers supply chain threats.

Yes

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.

N/A

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 a public cloud.

Yes

Section 10: Contractor Systems

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 (NIST SP 800-53: CA-2).(Base)

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 a public cloud.

No

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

Yes

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 a public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

No

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.

On September 8, 2014 GAO released a report titled "INFORMATION SECURITY: Agencies Need to Improve Oversight of Contractor Controls." This GAO report indicated that "the EPA did not always complete or update POA&Ms [Plan of Action and Milestones] for their contractor-operated systems. Specifically, the EPA could not provide an updated POA&M for one of the two systems reviewed. Without complete or up-to-date POA&Ms, agencies increase the risk that identified weaknesses will not be resolved in a timely fashion." Furthermore, the GAO report indicated the system assessments that EPA performed were not always effective.

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

Section 11: Security Capital Planning

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 SP 800-53: SA-2).**

Yes

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

Yes

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.**

N/A

Appendix A

Distribution

Office of the Administrator
Assistant Administrator for Environmental Information and Chief Information Officer
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Principal 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
Audit Follow-Up Coordinator, Office of Environmental Information