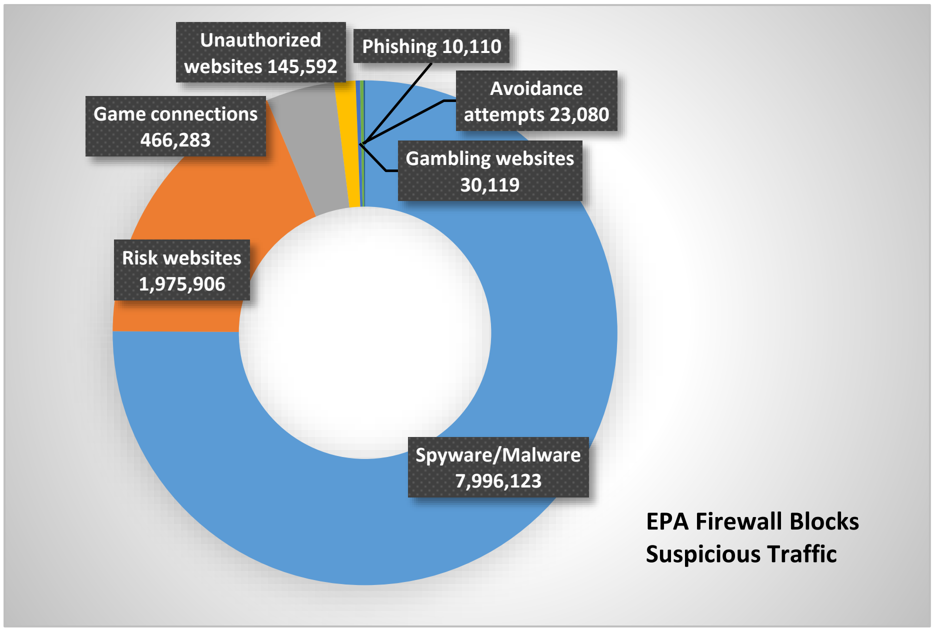
U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Information Technology

Fiscal Year 2015 Federal Information Security Modernization Act Report: Status of EPA's Information Security Program

Report No. 16-P-0039 November 16, 2015



Report Contributors:

Rudolph M. Brevard
Vincent Campbell
Eric K. Jackson, Jr.
Nii-Lantei Lamptey
Christina Nelson
Teresa Richardson

Abbreviations

DHS	U.S. Department of Homeland Security
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Modernization Act
OIG	Office of Inspector General

Cover image: OIG analysis of the EPA's network traffic blocked by the agency's firewall.

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

Learn more about our OIG Hotline.

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

16-P-0039
November 16, 2015

At a Glance

Why We Did This Review

The Office of Inspector General conducted this audit to evaluate the U.S. Environmental Protection Agency's (EPA's) compliance with the Federal Information Security Modernization Act (FISMA) of 2014 during fiscal year (FY) 2015.

In its FY 2015 budget, the EPA cites effectively leveraging technology as one of the key components central to the agency achieving its strategic goals. Protecting the confidentiality, integrity and availability of systems and data is necessary if the EPA plans to provide stakeholders access to accurate information to manage human health and environmental risks. As such, implementing an effective information security program is an underpinning process in achieving the EPA's goals.

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.

Listing of OIG reports.

Fiscal Year 2015 Federal Information Security Modernization Act Report: Status of EPA's Information Security Program

What We Found

The EPA fully met 60 percent (six of 10) of the information security areas evaluated using criteria specified by the FY 2015 Department of Homeland Security FISMA reporting metrics:

- Continuous Monitoring.
- Configuration Management.
- Incident Response and Reporting.
- Security Training.
- Remote Access Management.
- Contingency Planning.

The lack of a fully developed contractor systems program hinders the EPA in protecting its resources and data.

One metric—**Contractor Systems**—requires significant management attention to correct deficiencies noted in this area. Although the EPA has guidance in place for oversight of contractor systems, significant improvements are needed to (1) ensure contractors comply with required security controls, (2) maintain an accurate inventory of contractor systems, and (3) identify contractor systems that interface with the EPA systems.

For the three remaining metrics, management attention is needed to improve processes that potentially could place these areas at risk.

- **Identity and Access Management:** Improvements are needed in granting access to systems based on need and segregation of duties.
- **Risk Management:** Improvements are needed in tracking the performance of cloud service providers.
- **Plan of Action & Milestones:** Improvements are needed in ensuring that Plans of Actions & Milestones identify the resources and costs necessary to remediate vulnerabilities.

Appendix A contains the results of our analysis in accordance with the FISMA reporting instructions and EPA agreed with our results. We briefed EPA officials on the conclusion and, where appropriate, we updated our analysis and incorporated management's feedback. We made no recommendations for corrective actions related to the Contractor System significant deficiencies because these findings and the corresponding recommendations were disclosed in a prior Office of Inspector General report. The EPA indicated it completed two of the five prior report recommendations and the remaining three recommendations are open with corrective actions pending.

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

THE INSPECTOR GENERAL

MEMORANDUM

SUBJECT: Fiscal Year 2015 Federal Information Security Modernization Act Report:
Status of EPA's Information Security Program
Report No. 16-P-0039

FROM: Arthur A. Elkins Jr.

TO: Gina McCarthy, Administrator

This is our final report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This report contains findings and conclusions that meet the Federal Information Security Modernization Act reporting requirements prescribed by the Office of Management and Budget and Department of Homeland Security. This report represents the opinion of the OIG and does not necessarily represent the final EPA position.

The EPA office having primary oversight for areas evaluated in this report is the Office of Environmental Information.

Action Required

You are not required to provide a written response to this final report. In accordance with Office of Management and Budget Federal Information Security Modernization Act reporting instructions, we are forwarding this report to you for submission, along with the agency's required information, to the Director of the Office of Management and Budget.

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

Table of Contents

Appendices

Purpose

The U.S. Environmental Protection Agency (EPA), Office of Inspector General (OIG), conducted this audit to evaluate the EPA's compliance with the Federal Information Security Modernization Act (FISMA) of 2014 during fiscal year (FY) 2015.

Background

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems.

In its FY 2015 budget, the EPA cites effectively leveraging technology as one of the key components that is central to its strategy to protect public health and safeguard the environment. Implementing an effective information security program—focusing on protecting the confidentiality, integrity and availability of EPA data and systems—is key to the EPA being able to leverage technology and provide information to better manage human health and environmental risks.

Responsible Office

The Office of Environmental Information leads EPA's information management and information technology programs to provide the information, technology and services necessary to advance the protection of human health and the environment. Within the Office of Environmental Information, the EPA's Senior Agency Information Security Officer is responsible for developing, documenting, implementing and maintaining an agencywide information security program to protect EPA information and information systems. Additionally, the Senior Agency Information Security Officer ensures that the agencywide information security program is in compliance with FISMA and related information security laws, regulations, directives, policies and guidelines.

Scope and Methodology

We conducted our audit from June to October 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objectives.

Our testing consisted of a judgmental sample of active EPA systems with a data classification rating of moderate[1] and selected portions of the agency's information security program overseen by the EPA's Office of Environmental Information. We conducted our testing through inquiry of agency personnel, inspection of relevant documentation, and performance of security control testing. The testing of selected security controls covered areas designated within the U.S. Department of Homeland Security's (DHS's) *FY 2015 Inspector General Federal Information Security Management Act Reporting Metrics V1.1*, issued December 18, 2014; and *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.2*, issued June 19, 2015. We evaluated the EPA's continuous monitoring program against level one of the five possible maturity models. We did not evaluate the program against the criteria for the remaining levels the maturity model and are not reporting on the program's achievement of these levels.

Management agreed with the conclusions reported in Appendix A. We collected management's feedback on the analysis either verbally or through email. Due to the audit's broad scope and time constraints, we worked closely with the agency and briefed them on each portion of the DHS FISMA reporting metrics as the results were completed. As such, we updated our analysis and incorporated management feedback throughout the audit.

We made no recommendations for corrective actions related to the Contractor System significant deficiencies because these findings and the corresponding recommendations were disclosed in prior EPA OIG Report No. 15-P-0290, *Incomplete Contractor Systems Inventory and a Lack of Oversight Limit EPA's Ability to Facilitate IT Governance*, issued September 21, 2015. While EPA indicated it completed two of the five prior report recommendations, the three remaining recommendations are open with corrective actions pending.

There were no recommendations made in the FY 2014 FISMA report and no outstanding recommendations from prior years.

Results of Review

The EPA fully met 60 percent (six of 10) of the information security areas evaluated using criteria specified by the DHS FY 2015 FISMA reporting metrics. Our analysis disclosed the EPA established an agencywide information security program consistent with DHS criteria for the following six areas:

[1] Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004 identifies "MODERATE" as "A serious adverse effect to the loss of confidentiality, integrity, or availability which might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries."

- Continuous Monitoring
- Incident Response and Reporting
- Remote Access Management
- Configuration Management
- Security Training
- Contingency Planning

However, the EPA must take steps to significantly improve its processes for remediating deficiencies within the agency's **Contractor Systems** program. While the EPA has policies and procedures in place for the information security oversight of systems operated on the organization's behalf, the agency lacks effective processes to carry them out. In addition to evaluating the EPA's contractor systems program, we evaluated five additional components outlined in the DHS FISMA reporting metrics. As noted in table 1, the EPA successfully met only one of these five components.

Table 1. Results of evaluation of EPA's contractor system program

Area reviewed	Compliance with selected FISMA requirements
The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and compliant with FISMA requirements.	Not met
A complete inventory of systems operated on the organization's behalf by contractors or other entities.	Not met
The inventory identifies interfaces between these systems and organization-operated systems.	Not met
The organization requires appropriate agreements (e.g., Memorandums of Understanding, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.	Met
The inventory of contractor systems is updated at least annually.	Not met*
* We considered this area as "Not Met" because the EPA was unable to provide the OIG with a contractor system inventory by September 30, 2015, and no inventory existed.	

Source: OIG analysis.

For the remaining three information security areas, the agency partially complied with Identity and Access Management, Risk Management, and Plan of Action & Milestones programs. Process improvements are needed in the following:

- **Identity and Access Management:** The EPA needs improvement in its processes for (1) granting access to information systems based on needs and separation-of-duties and (2) terminating or deactivating access to information systems once access is no longer required.

- **Risk Management:** The EPA needs improvement in its processes for managing cloud system documentation to track the performance of the cloud service providers.

- **Plan of Action & Milestones:** The EPA needs improvement in its processes to ensure that resources and costs needed to remediate vulnerabilities are identified on the agency's network and connected devices.

Conclusion

While the EPA demonstrated it implemented a security program consistent with the majority of the selected FISMA criteria, the agency's reliance on contractors and other agencies to operate systems on its behalf puts the agency at risk due to ineffective oversight. As such, questions exist as to whether the EPA is doing all it can to protect the confidentiality, integrity and availability of externally operated information technology resources and stored data. This is essential to advancing the protection of human health and the environment.

Appendix A

Department of Homeland Security CyberScope Template

Inspector General

Section Report

2015

Annual FISMA Report

Environmental Protection Agency

Section 1: Continuous Monitoring Management

1.1 **Utilizing the ISCM maturity model definitions, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.**

1.1.1 **Please provide the D/A ISCM maturity level for the People domain.**

Ad Hoc (Level 1)

1.1.2 **Please provide the D/A ISCM maturity level for the Processes domain.**

Ad Hoc (Level 1)

1.1.3 **Please provide the D/A ISCM maturity level for the Technology domain**

Ad Hoc (Level 1)

1.1.4 **Please provide the D/A ISCM maturity level for the ISCM Program Overall.**

Ad Hoc (Level 1)

1.2 **Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model above.**

See Note

Comments: We have evaluated the EPA's Continuous Monitoring program against level one of the five level CM maturity model. We did not evaluate the program against the criteria for levels two through five of the model and are not reporting on the program's achievement of these levels. Therefore we can only state that the EPA program has achieved at least level one.

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?**

Yes

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

Yes

2.1.2 **Defined standard baseline configurations.**

Yes

Section 2: Configuration Management

2.1.3 **Assessments of compliance with baseline configurations.**

Yes

2.1.4 **Process for timely (as specified in organization policy or standards) remediation of scan result findings.**

Yes

2.1.5 **For Windows-based components, USGCB secure configuration settings are fully implemented (when available), and any deviations from USGCB baseline settings are fully documented.**

Yes

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

Yes

2.1.7 **Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI- 2).**

Yes

2.1.8 **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).**

Yes

2.1.9 **Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches (NIST SP 800-53: CM-3, SI-2).**

Yes

Comments: We evaluated the EPA's IT assets monitored for compliance by the agency's centralized managed tool.

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 an automated scanning capability?**

Yes

Comments: We evaluated the EPA's IT assets monitored for compliance by the agency's centralized managed tool.

Section 2: Configuration Management

2.3.1 Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented.

Yes

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 which 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 (HSPD 12, NIST SP 800-53, AC-2).

Yes

3.1.3 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

3.1.4 Organization has 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

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

No

3.1.6 Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. IP phones, faxes, printers).

Yes

3.1.7 Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy.

No

Section 3: Identity and Access Management

3.1.8 **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

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

Yes

4.1.4 **When applicable, reports to law enforcement and the agency Inspector General within established timeframes.**

Yes

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; OMB M-07-16, M-06-19).**

Yes

4.1.6 **Is capable of correlating incidents.**

Yes

4.1.7 **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

Section 4: Incident Response and Reporting

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 **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

5.1.2 **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

5.1.3 **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

5.1.4 **Has an up-to-date system inventory.**

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 and describes how the controls are employed within the information system and its environment of operation.**

Yes

5.1.7 **Implements the approved set of tailored baseline security controls specified in metric 5.1.6.**

Yes

Section 5: Risk Management

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

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

Yes

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

Yes

5.1.12 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

5.1.13 Security authorization package contains system security plan, security assessment report, POA&M, accreditation boundaries in accordance with government policies for organization information systems (NIST SP 800-18, 800-37).

Yes

5.1.14 The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.

No

5.1.15 For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems.

No

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

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.**

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

Comments: We evaluated whether EPA employees completed role-based training and did not test whether similar procedures existed for EPA contractors.

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.**

N/A

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 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 and provides adequate justification for missed 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 in terms of dollars (NIST SP 800-53: PM-3; 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: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 SP 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 **Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.**

Yes

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

Yes

8.1.7 **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

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

Yes

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

Yes

Section 8: Remote Access Management

8.1.10 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 and Business Process Analysis into the appropriate analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan (NIST SP 800-34).

Yes

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).

Yes

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 **Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for systems that require them (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

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

Yes

9.1.11 **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 for organization systems and services residing in a cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

No

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 other government agencies), including organization systems and services residing in a public, hybrid, or private 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 compliant with FISMA requirements, OMB policy, and applicable NIST guidelines (NIST SP 800-53: CA-2).**

No

10.1.3 **A complete inventory of systems operated on the organization’s behalf by contractors or other entities, (including other government agencies), including organization systems and services residing in public, hybrid, or private cloud.**

No

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

No

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.**

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.**

See Note.

Comments:

The following deficiencies were identified in the OIG’s report titled "Incomplete Contractor Systems Inventory and a Lack of Oversight Limit EPA’s Ability to Facilitate IT Governance,” 15-P-0290, published on September 21, 2015:

1) Agency officials were unaware of which systems or services are required by the EPA's System Life Cycle Management Procedures.

2) Officials were also unaware of which stage of the system life cycle to enter contractor systems into the EPA's authoritative registry. The registry also lacked information on 81 internal EPA contractor-supported systems.

3) Personnel with oversight responsibilities were unaware of requirements in the EPA’s information security procedures. EPA contractors did not (1) conduct required annual security assessments, (2) provide security assessment results to the EPA, and (3) establish a required incident response capability.

Appendix B

Distribution

Office of the Administrator
Chief Information Officer, 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 Public Affairs
Principal Deputy Assistant Administrator and Deputy Chief Information Officer,
Office of 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