



U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

*Compliance with the law  
Operating efficiently and effectively*

## EPA's Information Security Program Is Established, but Improvements Are Needed to Strengthen Its Processes

Report No. 18-P-0031

October 30, 2017



## Report Contributors:

Rudolph M. Brevard  
Vincent Campbell  
Nancy Dao  
Eric K. Jackson Jr.  
Scott Sammons  
Tessa Waters  
Ben Beeson

## Abbreviations

EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG	Inspector General
OIG	Office of Inspector General
U.S.C.	United States Code

**Cover image:** Cybersecurity Framework. (EPA OIG graphic)

**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](mailto: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](http://www.epa.gov/oig)

Subscribe to our [Email Updates](#)  
Follow us on Twitter [@EPAoig](#)  
Send us your [Project Suggestions](#)



# At a Glance

## Why We Did This Review

The Office of Inspector General conducted this audit to assess the U.S. Environmental Protection Agency's (EPA's) compliance with the Federal Information Security Modernization Act of 2014 (FISMA) during fiscal year (FY) 2017.

The Inspector General (IG) FISMA reporting metrics outline five maturity levels for IGs to rate their agency's information security programs:

- Level 1 – Ad-Hoc
- Level 2 – Defined
- Level 3 – Consistently Implemented
- Level 4 – Managed and Measurable
- Level 5 – Optimized

The maturity model is a tool that summarizes an agency's information security program and outlines activities to improve the program.

We reported our audit results using the CyberScope system developed by the U.S. Department of Homeland Security.

### This report addresses the following:

- *Compliance with the law.*
- *Operating efficiently and effectively.*

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

Listing of [OIG reports](#).

## ***EPA's Information Security Program Is Established, but Improvements Are Needed to Strengthen Its Processes***

### What We Found

The EPA has an effective information security program and has completed all the requirements to achieve a Level 3 (Consistently Implemented) maturity level for the five security functions and related domains defined within the FY 2017 IG FISMA reporting metrics:

**Although the EPA has an effective information security program, management emphasis is needed to achieve a higher level of maturity for the agency's information security program.**

1. Identify – Risk Management.
2. Protect – Configuration Management, Identity and Access Management, and Security Training.
3. Detect – Information Security Continuous Monitoring.
4. Respond – Incident Response.
5. Recover – Contingency Planning.

We tested whether the EPA developed policies, procedures and strategies for each area within the IG FISMA reporting metrics. We also analyzed EPA management's self-assessments that contained assertions and additional information on whether the agency implemented processes and practices consistent with the specified security functions and related domains. In addition, we evaluated prior audit work to determine whether the self-assessments were consistent with our audit findings.

We concluded that the EPA defined policies, procedures and strategies for each security function and related domains. EPA management also provided sufficient evidence that the agency implemented a majority of processes and practices consistent with maturity model Level 3 (Consistently Implemented). However, we found substantial weaknesses in the EPA's information security training program related to how the agency verifies whether contractor personnel with significant information security responsibilities comply with specialized security training requirements.

Appendix A documents the results for the FY 2017 IG FISMA reporting metrics. We worked closely with EPA officials and briefed them on the results. We made no recommendations based on our analysis. The EPA agreed with our conclusions.



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

THE INSPECTOR GENERAL

October 30, 2017

**MEMORANDUM**

**SUBJECT:** EPA's Information Security Program Is Established,  
but Improvements Are Needed to Strengthen Its Processes  
Report No. 18-P-0031

**FROM:** Arthur A. Elkins Jr.

A handwritten signature in black ink, appearing to read "Arthur A. Elkins Jr.", is written over the printed name.

**TO:** Scott Pruitt, 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). The project number for this audit was OA-FY17-0204. This report contains conclusions that meet the Federal Information Security Modernization Act of 2014 reporting requirements as prescribed by the Office of Management and Budget and U.S. 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 the primary oversight for the 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 the Office of Management and Budget Federal Information Security Modernization Act reporting instructions, we are forwarding this report, 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](http://www.epa.gov/oig).

# *Table of Contents*

---

Purpose.....	1
Background.....	1
Responsible Office.....	2
Scope and Methodology.....	3
Results of Review.....	4
Conclusion.....	6

## **Appendices**

- A Department of Homeland Security CyberScope Template
- B Information Security Reports Issued in FY 2017
- C Distribution

## Purpose

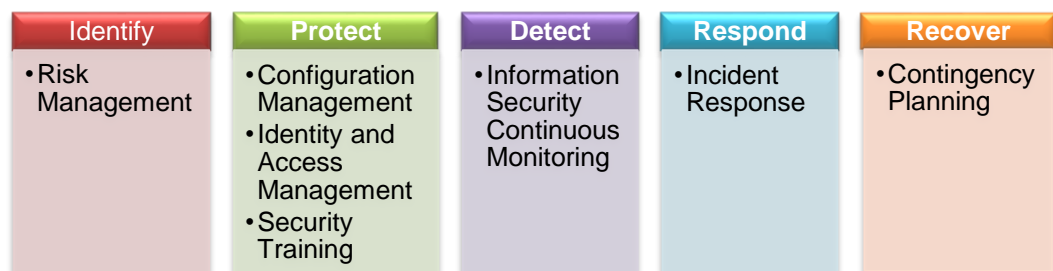
The U.S. Environmental Protection Agency (EPA) Office of Inspector General (OIG) conducted this audit to evaluate the EPA's compliance with the Federal Information Security Modernization Act of 2014 (FISMA) during fiscal year (FY) 2017.

## Background

Under FISMA (44 U.S.C. §3554 (a)(1)(A)(i) and (ii)), 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.

The FY 2017 Inspector General (IG) FISMA reporting metrics identified seven domains within the five security functions defined in the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity. Each security function contains at least one corresponding domain of an agency's information security program, as shown in Figure 1. The National Institute of Standards and Technology cybersecurity framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise.

**Figure 1: Cybersecurity framework security functions and domains**



Source: FY 2017 IG FISMA of 2014 reporting metrics.

The IG FISMA reporting metrics provide guidance for assessing the maturity of controls to address those risks. This year's FISMA metrics represents a significant departure from prior year's reporting metrics. This year, the Office of Management and Budget introduced a new maturity model rating system for three of the five functions (Identify, Protect, and Recover). The Office of Management and Budget also reorganized the model itself to make it more intuitive. This eliminates our ability to compare this year's results to prior ratings of the security functions. The effectiveness of the information security program is based on a maturity model spectrum, in which levels 1 and 2 describe whether agencies have developed policies and procedures and levels 3 to 5 describe the extent to which the agencies have institutionalized those policies and procedures. Figure 2 details

the five maturity model levels, with Level 5 – “Optimized” being the highest maturity level an organization can achieve.

**Figure 2: Maturity model levels**



Source: FY 2017 IG FISMA of 2014 reporting metrics.

Within the context of the maturity model, Level 4 – “Managed and Measurable” represents an effective level of security at the domain, function and overall program level. In addition, the FY 2017 IG FISMA reporting metrics grant IGs the discretion to rate the agency’s information security program at a different maturity level than what has been calculated by the CyberScope system. The reporting metrics stated that the rationale is to provide greater flexibility when assessing the agency’s information security program.

## Responsible Office

The Office of Environmental Information leads the 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 Chief Information Security Officer is responsible for the EPA’s information security program. Additionally, the Chief Information Security Officer is responsible for developing an agencywide information security program that

complies with FISMA and related information security laws, regulations, directives, policies and guidelines.

## Scope and Methodology

We conducted our performance audit from May to October 2017 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.

We conducted our testing through inquiries of agency personnel, inspection of relevant documentation and leveraging of current OIG information security audit work related to the Cybersecurity Framework Security Functions and domains. We also reviewed FY 2017 audit reports issued by the U.S. Government Accountability Office and the EPA OIG to identify any issues related to the security function areas.

The FY 2017 IG FISMA reporting metrics require IGs to provide three separate assessments of their agency's information security program. The first assessment requires IGs to evaluate their agency's information security program with respect to 54 questions related to the five security functions and related domains defined within the IG FISMA reporting metrics. The CyberScope system, which is used to report our assessment results, calculates a maturity model level for each security function based on the IG responses to the 54 questions. The second assessment requires IGs to provide additional information about the effectiveness of their agency's information security program that was not asked by the questions contained in the IG FISMA reporting metrics. The third assessment requires IGs to provide an overall self-assessment rating of Effective or Not Effective for its agency's information security program. In providing these three assessments, we conducted the following audit work to reach our conclusions for each required assessment:

- **IG FISMA Reporting Metrics Questions:** For each security function and related domain, we evaluated whether the EPA took the necessary action to complete Level 1 (Ad-Hoc) of the IG FISMA reporting metrics maturity model. For each level, agencies are required to meet specific steps to achieve that level and be considered reaching the next level within the maturity model. As such, we evaluated whether EPA policies, procedures and strategies met the Level 1 requirements for each security function and related domain. If the policies, procedures and strategies were formalized and documented, we rated the EPA at Level 2 (Defined). If the EPA did not meet all the requirements, we rated the agency at Level 1 (Ad Hoc) because that is the minimum level.



- **Additional Information About the EPA’s Security Program:** For each security function and related domain, we used the control self-assessment methodology<sup>1</sup> to collect and evaluate EPA management’s information on the effectiveness of the agency’s information security program. We reviewed the provided information to determine whether the documents were relevant and reasonably supported the agency’s assertions. We also relied upon audit work performed from FYs 2015 through 2017 to further assess whether management’s assertions were consistent with our conclusions.
- **Overall Self-Assessment Rating:** We based our overall conclusion on the analysis of the collected audit documentation and whether the EPA:
  - Documented that policies, procedures and strategies were consistent with the IG FISMA reporting metrics questions.
  - Provided documentation of its information security practices and that activities met requirements consistent with the security functions and related domains outlined within the IG FISMA reporting metrics.
  - Implemented processes and activities, based on prior audit work, that were consistent with the security functions and related domains specified within the IG FISMA reporting metrics, even though weaknesses may have existed and the OIG made recommendations for management to improve controls.

## Results of Review

The EPA has an effective information security program. Based on our analysis of EPA material and the additional documentation provided by EPA representatives, we concluded that the EPA took sufficient steps to complete the requirements specified within the FY 2017 IG FISMA reporting metrics to reach Level 3 (Consistently Implemented) of the FISMA maturity model.

We concluded that the EPA fully defined its policies, procedures and strategies and met the requirements of the security functions and related security domains outlined within the IG FISMA reporting metrics. The EPA asserted that it has fully implemented processes and activities consistent with the security functions and related domains specified within the IG FISMA reporting metrics, and provided artifacts and other documentation to support their assertions. Based on our analysis of this documentation and comparison of management’s assertions against prior audit work, we concluded that the evidence supported management’s assertions.

---

<sup>1</sup> According to the Institute of Internal Auditors, control self-assessment is a technique that allows personnel directly involved in the business process to participate in assessing the organization’s risk management and control processes. Audit teams can use control self-assessment results to gather relevant information about risk and controls.

EPA management provided sufficient evidence that the agency implemented a majority of processes and practices consistent with the 54 questions outlined in the FY 2017 IG FISMA reporting metrics. We rated the EPA’s information security function areas at maturity Level 3 on the IG FISMA reporting metrics maturity model, as shown in Table 1.

**Table 1: Maturity level of EPA’s information security function areas**

Security Function	Maturity Level
1. Identify	Level 3: Consistently Implemented
2. Protect	Level 3: Consistently Implemented
3. Detect	Level 3: Consistently Implemented
4. Respond	Level 3: Consistently Implemented
5. Recover	Level 3: Consistently Implemented

Source: Results of OIG analyses of EPA’s self-assessments.

However, the EPA indicated that it has not implemented some activities associated with the security functions. For example:

- Risk Management:** The EPA has not consistently implemented a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization’s network with the detailed information necessary for tracking and reporting.
- Identity and Access Management:** EPA has not fully implemented an Identity, Credential and Access Management strategy to guide its Identity, Credential and Access Management processes and activities.

We also found substantial weaknesses in the EPA’s information security training program related to how the agency verifies that contractor personnel with significant information security responsibilities comply with specialized security training requirements. The OIG issued Report No. [17-P-0344](#), *EPA Lacks Processes to Validate Whether Contractors Receive Specialized Role-Based Training for Network and Data Protection*, which noted that the EPA is unaware as to whether information security contractors possess the skills and training needed to protect the agency’s information, data and network from security breaches. As such, we rated a question within the Protect security function in the IG FISMA reporting metrics on specialized training for personnel with significant information security responsibilities at Level – 1 (Ad-hoc).

We worked closely with the agency representatives and briefed them on each portion of the IG FISMA reporting metrics as the results were completed. We collected management’s feedback on our analysis either verbally or through email. Where appropriate, we updated our analysis and incorporated management’s feedback. Appendix A contains the detailed results of our analysis.

Management agreed with our conclusions. Appendix B contains a listing of significant information security audit reports published in FY 2017.

## **Conclusion**

Although the EPA has an effective information security program, management emphasis is needed to achieve a higher level of maturity for the agency's information security program.

***Department of Homeland Security  
CyberScope Template***

# Inspector General

Section Report

2017

Annual FISMA  
Report

## Environmental Protection Agency

## Function 1: Identify - Risk Management

- 1 Does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800-53: CA-3 and PM-5; OMB M-04-25; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4)?

**Defined (Level 2)**

**Comments:** See comment for Question 13.2.

- 2 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2)?

**Defined (Level 2)**

**Comments:** See comment for Question 13.2.

- 3 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?

**Defined (Level 2)**

**Comments:** See comment for Question 13.2.

- 4 To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; and FIPS 199)?

**Defined (Level 2)**

**Comments:** See comment for Question 13.2.

- 5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that include the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST 800-39; NIST 800-53: PM-8, PM-9; CSF: ID.RM-1 – ID.RM-3; OMB A-123; CFO Council ERM Playbook)?

**Defined (Level 2)**

**Comments:** See comment for Question 13.2.

## Function 1: Identify - Risk Management

- 6 Has the organization defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture to provide a disciplined and structured methodology for managing risk (NIST 800-39; FEA; NIST 800-53: PL-8, SA-3, and SA-8)?

**Defined (Level 2)**

**Comments:** See comment for Question 13.2.

- 7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST 800-39: Section 2.3.1 and 2.3.2; NIST 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2, OMB A-123, CFO Council ERM Playbook)?

**Defined (Level 2)**

**Comments:** See comment for Question 13.2.

- 8 To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53: CA-5; OMB M-04-25)?

**Defined (Level 2)**

**Comments:** See comment for Question 13.2.

- 9 To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing
- (i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework
  - (ii) internal and external asset vulnerabilities, including through vulnerability scanning,
  - (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and
  - (iv) selecting and implementing security controls to mitigate system-level risks (NIST 800--37; NIST 800-39; NIST 800--53: PL-2, RA-1; NIST 800-30; CSF:ID.RA-1 – 6)?

**Defined (Level 2)**

**Comments:** See comment for Question 13.2.

- 10 To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123)?

**Defined (Level 2)**

**Comments:** See comment for Question 13.2.

## Function 1: Identify - Risk Management

- 11 To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (FAR Case 2007--004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, 52.239-1; President's Management Council; NIST 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2017 CIO FISMA Metrics: 1.7, 1.8)?

### Defined (Level 2)

**Comments:** See comment for Question 13.2.

- 12 To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?

### Defined (Level 2)

**Comments:** See comment for Question 13.2.

- 13.1 Please provide the assessed maturity level for the agency's Identify - Risk Management function.

### Consistently Implemented (Level 3)

**Comments:** See comment for Question 13.2.



## Function 1: Identify - Risk Management

- 13.2 Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

**The EPA has an effective information security program. Based on our analysis of EPA material and the additional documentation provided by EPA representatives, we concluded that the EPA took sufficient steps to complete the requirements specified within the FY 2017 IG FISMA reporting metrics to reach Level 3 (Consistently Implemented) of the FISMA maturity model.**

**However, the EPA indicated that it has not implemented some activities associated with the security functions. For example:**

**The EPA has not consistently implemented a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting.**

**Comments:**

We limited our testing to determine whether the agency possessed the noted policies, procedures and strategies required for each metric under the function area. If the policies, procedures and strategies were formalized and documented we rated the agency at level 2 (Defined). If not, we rated the agency at level 1 (Ad Hoc). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

**Calculated Maturity Level - Defined (Level 2)**

## Function 2A: Protect - Configuration Management

- 14 To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800- 53: CM-1; SP 800-128: Section 2.4)?

**Defined (Level 2)**

**Comments:**

See comment in Question 22.

- 15 To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate location within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contracted systems (NIST 800--128: Section 2.3.2; NIST 800--53: CM-9)?

**Defined (Level 2)**

**Comments:**

See comment in Question 22.

## Function 2A: Protect - Configuration Management

16 To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53: CM-1; NIST 800-128: 2.2.1)

**Defined (Level 2)**

**Comments:** See comment in Question 22.

17 To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53: CM-2, CM-8; FY 2017 CIO FISMA Metrics: 1.4, 1.5, and 2.1; CSF: ID.DE.CM-7)?

**Defined (Level 2)**

**Comments:** See comment in Question 22.

18 To what extent does the organization utilize configuration settings/common secure configurations for its information systems (NIST SP 800-53: CM-6, CM-7, and SI-2; FY 2017 CIO FISMA Metrics: 2.2; SANS/CIS Top 20 Security Controls 3.7)?

**Defined (Level 2)**

**Comments:** See comment in Question 22.

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53: CM-3, SI-2; NIST 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20 Control 4.5; and DHS Binding Operational Directive 15-01)?

**Defined (Level 2)**

**Comments:** See comment in Question 22.

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (FY 2017 CIO Metrics: 2.26, 2.27, 2.29; OMB M-08-05)?

**Defined (Level 2)**

**Comments:** See comment in Question 22.

21 To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST 800-53: CM--2, CM-3)?

**Defined (Level 2)**

**Comments:** See comment in Question 22.

**Function 2A: Protect - Configuration Management**

22 Provide any additional information on the effectiveness (positive or negative) of the organization’s configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?

**The EPA has an effective information security program. Based on our analysis of EPA material and the additional documentation provided by EPA representatives, we concluded that the EPA took sufficient steps to complete the requirements specified within the FY 2017 IG FISMA reporting metrics to reach Level 3 (Consistently Implemented) of the FISMA maturity model.**

**(a) Stakeholders have adequate resources (people, processes and technology) to consistently implement information system configuration management activities.**

**(b) The EPA has developed a Configuration Management Policy to establish an Agency-wide Configuration Management Program.**

**(c) The EPA consistently implements its policies and procedures for managing the configurations of its information systems. Further, the organization utilizes lessons learned sessions to make improvements to its policies and procedures.**

**(d) The EPA consistently records, implements and maintains baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures.**

**(e) The EPA consistently implements, assesses and maintains secure configuration settings for its information systems based on least functionality.**

**(f) The EPA consistently implements its flaw remediation policies, procedures and processes and ensures that patches, hotfixes, service packs and anti-virus/malware software updates are identified and installed.**

**Comments:**

We limited our testing to determine whether the agency possessed the noted policies, procedures and strategies required for each metric under the function area. If the policies, procedures and strategies were formalized and documented we rated the agency at level 2 (Defined). If not, we rated the agency at level 1 (Ad Hoc). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

**Calculated Maturity Level - Defined (Level 2)**

**Function 2B: Protect - Identity and Access Management**

## Function 2B: Protect - Identity and Access Management

23 To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST 800-53: AC-1, IA-1, PS-1; and the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

**Defined (Level 2)**

**Comments:** See comment for Question 32.

24 To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?

**Defined (Level 2)**

**Comments:** See comment for Question 32.

25 To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 27 through 31) (NIST 800-53: AC-1 and IA--1; Cybersecurity Strategy and Implementation Plan (CSIP); and SANS/CIS Top 20: 14.1)?

**Defined (Level 2)**

**Comments:** See comment for Question 32.

26 To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53: PS-2, PS- 3; and National Insider Threat Policy)?

**Defined (Level 2)**

**Comments:** See comment for Question 32.

27 To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non- privileged users) that access its systems are completed and maintained (NIST SP 800--53: AC-8, PL-4, and PS-6)?

**Defined (Level 2)**

**Comments:** See comment for Question 32.

28 To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800--53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

**Defined (Level 2)**

**Comments:** See comment for Question 32.

## Function 2B: Protect - Identity and Access Management

29 To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800--53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

**Defined (Level 2)**

**Comments:**

See comment for Question 32.

30 To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2017 CIO FISMA metrics: Section 2; NIST SP 800-53: AC-1, AC-2 (2), AC-17; CSIP)?

**Defined (Level 2)**

**Comments:**

See comment for Question 32.

31 To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53: AC--17, SI-4; and FY 2017 CIO FISMA Metrics: Section 2)?

**Defined (Level 2)**

**Comments:**

See comment for Question 32.

## Function 2B: Protect - Identity and Access Management

32 Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?

**The EPA has an effective information security program. Based on our analysis of EPA material and the additional documentation provided by EPA representatives, we concluded that the EPA took sufficient steps to complete the requirements specified within the FY 2017 IG FISMA reporting metrics to reach Level 3 (Consistently Implemented) of the FISMA maturity model.**

**However, the EPA indicated that it has not implemented some activities associated with the security functions. For example:**

**The EPA has not fully implemented an Identity, Credential and Access Management strategy to guide its Identity, Credential and Access Management processes and activities.**

**Comments:**

We limited our testing to determine whether the agency possessed the noted policies, procedures and strategies required for each metric under the function area. If the policies, procedures and strategies were formalized and documented we rated the agency at level 2 (Defined). If not, we rated the agency at level 1 (Ad Hoc). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

**Calculated Maturity Level - Defined (Level 2)**

## Function 2C: Protect - Security Training

33 To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST 800-53: AT-1; and NIST SP 800-50)?

**Defined (Level 2)**

**Comments:**

See comment for Question 39.2.

## Function 2C: Protect - Security Training

- 34 To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST 800-53: AT-2 and AT-3; NIST 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181 (Draft); and CIS/SANS Top 20: 17.1)?

### Defined (Level 2)

**Comments:** See comment for Question 39.2.

- 35 To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST 800--53: AT-1; NIST 800-50: Section 3))

### Defined (Level 2)

**Comments:** See comment for Question 39.2.

- 36 To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity questions 37 and 38 below) (NIST 800-53: AT-1 through AT-4; and NIST 800-50)

### Defined (Level 2)

**Comments:** See comment for Question 39.2.

- 37 To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: Awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST 800-53: AT-2; FY 17 CIO FISMA Metrics: 2.23; NIST 800-50: 6.2; SANS Top 20: 17.4)

### Defined (Level 2)

**Comments:** See comment for Question 39.2.

## Function 2C: Protect - Security Training

38 To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST 800-53: AT-3 and AT-4; FY 17 CIO FISMA Metrics: 2.23)?

### Ad Hoc (Level 1)

**Comments:**

The OIG issued a report on July 31, 2017, that documented that the EPA has not developed processes to validate that contractors have completed specialized (role-based) training.

39.1 Please provide the assessed maturity level for the agency's Protect - Configuration Management/Identity and Access Management/Security Training (Functions 2A - 2C).

### Consistently Implemented (Level 3)

**Comments:**

See comments for Questions 22, 32 and 39.2

39.2 Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?

**The EPA has an effective information security program. Based on our analysis of EPA material and the additional documentation provided by EPA representatives, we concluded that the EPA took sufficient steps to complete the requirements specified within the FY 2017 IG FISMA reporting metrics to reach Level 3 (Consistently Implemented) of the FISMA maturity model.**

**However, we also found weaknesses in the EPA's information security training program related to how the agency verifies contractor personnel with significant information security responsibilities comply with specialized security training requirements.**

**Comments:**

We limited our testing to determine whether the agency possessed the noted policies, procedures and strategies required for each metric under the function area. If the policies, procedures and strategies were formalized and documented we rated the agency at level 2 (Defined). If not, we rated the agency at level 1 (Ad Hoc). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

**Calculated Maturity Level - Defined (Level 2)**

## Function 3: Detect - ISCM



### Function 3: Detect - ISCM

40 To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM (NIST SP 800-137: Sections 3.1 and 3.6)?

**Defined (Level 2)**

**Comments:** See comment for Question 45.2.

41 To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53: CA-7). (Note: The overall maturity level should take into consideration the maturity of question 43)

**Defined (Level 2)**

**Comments:** See comment for Question 45.2.

42 To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53: CA-1; NIST SP 800-137; and FY 2017 CIO FISMA Metrics)?

**Defined (Level 2)**

**Comments:** See comment for Question 45.2.

43 How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800-137: Section 2.2; NIST SP 800-53: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?

**Defined (Level 2)**

**Comments:** See comment for Question 45.2.

44 How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?

**Defined (Level 2)**

**Comments:** See comment for Question 45.2.

45.1 Please provide the assessed maturity level for the agency's Detect - ISCM function.

**Consistently Implemented (Level 3)**

**Comments:** See comment for Question 45.2.

### Function 3: Detect - ISCM

45.2 Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?

**The EPA has an effective information security program. Based on our analysis of EPA material and the additional documentation provided by EPA representatives, we concluded that the EPA took sufficient steps to complete the requirements specified within the FY 2017 IG FISMA reporting metrics to reach Level 3 (Consistently Implemented) of the FISMA maturity model.**

**(a) The EPA's information security continuous monitoring policies and procedures have been consistently implemented for the specified areas. The EPA also consistently captures lessons learned to make improvements to the information security continuous monitoring policies and procedures. The EPA has ensured continuous monitoring is consistently implemented by using the authorization-to-operate package review process to provide oversight of the assessment process. This process ensures system control effectiveness is documented in the Agency's repository system and plan of action and milestones are created to track unmitigated weaknesses.**

**(b) The EPA has consistently implemented its processes for performing ongoing security control assessments, granting system authorizations and monitoring security controls. All security control classes (management, operational, technical) and types (common, hybrid and system-specific) are monitored and assessed on a three-year cycle.**

**Comments:**

We limited our testing to determine whether the agency possessed the noted policies, procedures and strategies required for each metric under the function area. If the policies, procedures and strategies were formalized and documented we rated the agency at level 2 (Defined). If not, we rated the agency at level 1 (Ad Hoc). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

**Calculated Maturity Level - Defined (Level 2)**

### Function 4: Respond - Incident Response

46 To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53: IR-1; NIST 800-61 Rev. 2; FY 2017 CIO FISMA Metrics: 4.1, 4.3, and 4.6)? (Note: The overall maturity level should take into consideration the maturity of questions 48 - -52)

**Defined (Level 2)**

**Comments:**

See comment for Questions 53.2.

## Function 4: Respond - Incident Response

47 To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-16-03; OMB M-16-04; FY 2017 CIO FISMA Metrics: 1.6 and 4.5; and US-CERT Federal Incident Notification Guidelines)?

**Defined (Level 2)**

**Comments:** See comment for Questions 53.2.

48 How mature are the organization's processes for incident detection and analysis (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; US- CERT Incident Response Guidelines)?

**Defined (Level 2)**

**Comments:** See comment for Questions 53.2.

49 How mature are the organization's processes for incident handling (NIST 800-53: IR-4)?

**Defined (Level 2)**

**Comments:** See comment for Questions 53.2.

50 To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-16-03; NIST 800-53: IR-6; US-CERT Incident Notification Guidelines)?

**Defined (Level 2)**

**Comments:** See comment for Questions 53.2.

51 To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents and enter into contracts, as appropriate, for incident response support (FY 2017 CIO FISMA Metrics: 4.4; NIST SP 800-86)?

**Defined (Level 2)**

**Comments:** See comment for Questions 53.2.

## Function 4: Respond - Incident Response

52 To what degree does the organization utilize the following technology to support its incident response program?

- Web application protections, such as web application firewalls
- Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools
- Aggregation and analysis, such as security information and event management (SIEM) products
- Malware detection, such as antivirus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2)

### Defined (Level 2)

**Comments:** See comment for Questions 53.2.

53.1 Please provide the assessed maturity level for the agency's Respond - Incident Response function.

### Consistently Implemented (Level 3)

**Comments:** See comment for Questions 53.2.

## Function 4: Respond - Incident Response

53.2 Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?

**The EPA has an effective information security program. Based on our analysis of EPA material and the additional documentation provided by EPA representatives, we concluded that the EPA took sufficient steps to complete the requirements specified within the FY 2017 IG FISMA reporting metrics to reach Level 3 (Consistently Implemented) of the FISMA maturity model.**

**(a) The EPA consistently utilizes its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis and prioritization. In addition, the organization consistently implements and analyzes precursors and indicators generated by the following technologies: intrusion detection/prevention, security information and event management, antivirus and antispam software, and file integrity checking software.**

**(b) The EPA consistently implements its containment strategies, incident eradication processes, processes to remediate vulnerabilities, and recovers system operations.**

**Comments:**

We limited our testing to determine whether the agency possessed the noted policies, procedures and strategies required for each metric under the function area. If the policies, procedures and strategies were formalized and documented we rated the agency at level 2 (Defined). If not, we rated the agency at level 1 (Ad Hoc). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

**Calculated Maturity Level - Defined (Level 2)**

## Function 5: Recover - Contingency Planning

54 To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST 800-53: CP-1 and CP-2; NIST 800-34; NIST 800-84; FCD-1: Annex B)?

**Defined (Level 2)**

**Comments:**

See comment for Question 61.2.

## Function 5: Recover - Contingency Planning

55 To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate? (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 56-60) (NIST SP 800-34; NIST SP 800--161).

**Defined (Level 2)**

**Comments:** See comment for Question 61.2.

56 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST 800-53: CP-2; NIST 800--34, Rev. 1, 3.2, FIPS 199, FCD--1, OMB M-17-09)?

**Defined (Level 2)**

**Comments:** See comment for Question 61.2.

57 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST 800-53: CP-2; NIST 800-34)?

**Defined (Level 2)**

**Comments:** See comment for Question 61.2.

58 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST 800-34; NIST 800-53: CP-3, CP-4)?

**Defined (Level 2)**

**Comments:** See comment for Question 61.2.

59 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST 800--53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD1; NIST CSF: PR.IP- 4; and NARA guidance on information systems security records)?

**Defined (Level 2)**

**Comments:** See comment for Question 61.2.

60 To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST 800-53: CP-2, IR-4)?

**Defined (Level 2)**

**Comments:** See comment for Question 61.2.

## Function 5: Recover - Contingency Planning

61.1 Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.

### Consistently Implemented (Level 3)

**Comments:**

See comment for Question 61.2.

61.2 Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?

**The EPA has an effective information security program. Based on our analysis of EPA material and the additional documentation provided by EPA representatives, we concluded that the EPA took sufficient steps to complete the requirements specified within the FY 2017 IG FISMA reporting metrics to reach Level 3 (Consistently Implemented) of the FISMA maturity model.**

**(a) The EPA has established appropriate teams that are ready to implement their information system contingency planning strategies. Stakeholders and teams have adequate resources (people, processes and technology) to effectively implement system contingency planning activities. The EPA mandates each system must have a contingency plan which goes through an annual review/update process.**

**(b) The EPA incorporates the results of organizational and system level business impact analyses into strategy and plan development efforts consistently. System level business impact analyses are integrated with the organizational level business impact analysis and include: (1) characterization of all system components, determination of missions/business processes and recovery criticality, (2) identification of resource requirements, and (3) identification of recovery priorities for system resources.**

**Comments:**

We limited our testing to determine whether the agency possessed the noted policies, procedures and strategies required for each metric under the function area. If the policies, procedures and strategies were formalized and documented we rated the agency at level 2 (Defined). If not, we rated the agency at level 1 (Ad Hoc). However, we did not conduct additional testing to determine whether the agency implemented the noted policies, procedures and strategies and we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

### Calculated Maturity Level - Defined (Level 2)

**Comments:**

See comment for F.02.

## Function 0: Overall

## Function 0: Overall

0.1 Please provide an overallIG self-assessment rating (Effective/Not Effective)

### Effective

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

**The EPA has an effective information security program. We concluded that the EPA fully defined its policies, procedures and strategies to meet the requirements of the security functions and related domains outlined in the IG FISMA reporting metrics. The EPA asserted that it has fully implemented processes and activities consistent with the IG FISMA reporting metrics and provided artifacts and other documentation to support their assertions. Based on our analysis of this documentation and comparison of management's assertions against prior audit work, we concluded the evidence supported management's assertions. We worked closely with EPA representatives and briefed them on each portion of the IG FISMA reporting metrics as the results were completed; collected management's feedback on our analysis; and, where appropriate, updated our analysis to incorporate management's feedback. We concluded that the EPA took sufficient steps to complete the requirements in order to reach Level 3 (Consistently Implemented) of the FISMA maturity model. Management agreed with our conclusions.**

## APPENDIX A: Maturity Model Scoring

### Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	12
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0



### Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0
Defined	8
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

### Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	9
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

### Function 2C: Protect - Security Training

Function	Count
Ad-Hoc	1
Defined	5
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

### Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	5
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

### Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	7
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

### Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	7
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

Function	Defined (Level 2)	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management		Consistently Implemented (Level 3)	See comment for Question 13.2
Function 2: Protect - Configuration Management / Identity Management / Security Training	Defined (Level 2)	Consistently Implemented (Level 3)	See comments for Questions 22, 32 and 39.2
Function 3: Detect - ISCM	Defined (Level 2)	Consistently Implemented (Level 3)	See comment for Question 45.2.
Function 4: Respond - Incident Response	Defined (Level 2)	Consistently Implemented (Level 3)	See comment for Questions 53.2.
Function 5: Recover - Contingency Planning	Defined (Level 2)	Consistently Implemented (Level 3)	See comment for Question 61.2.
Overall	Not Effective	Effective	See comment for F.02.

## ***Information Security Reports Issued in FY 2017***

The EPA OIG issued the following reports in FY 2017 that included recommendations regarding different areas within the EPA's information security program:

- **Report No. [17-P-0344](#), *EPA Lacks Processes to Validate Whether Contractors Receive Specialized Role-Based Training for Network and Data Protection*, dated July 31, 2017.** We reported that the EPA is unaware as to whether information security contractors possess the skills and training needed to protect the agency's information, data and network from security breaches. In addition, the EPA did not report contractor training status in its FYs 2015 and 2016 Chief Information Officer's Annual FISMA reports submitted to the Office of Management and Budget. The agency also has insufficient information to manage risks to its data and network. We made four recommendations, and EPA officials agreed with the final recommendations along with completing one of the four recommendations. The EPA indicated in the agency's Management Audit Tracking System that it plans to complete all corrective actions for the remaining recommendations by October 31, 2019.
- **Report No. [17-P-0205](#), *Controls Needed to Track Changes to EPA's Compass Financials Data*, dated May 8, 2017.** We reported that the Office of the Chief Financial Officer needed to strengthen internal controls to certify that any changes made to the Compass Financials application are implemented based on management approval. Specifically, the Office of the Chief Financial Officer lacked documentation that supports the approval and verification of direct modifications made to the Compass database. The Office of the Chief Financial Officer also lacked procedures for handling emergency or unscheduled configuration changes made to financial information systems. We made three recommendations, and the EPA took actions to address the identified weaknesses. All three recommendations are closed with corrective actions completed.
- **Report No. [17-P-0062](#), *Congressionally Requested Audit: EPA Needs to Improve Processes for Preserving Text Messages as Federal Records*, dated December 21, 2016.** We reported that we did not find instances where the EPA used text messaging to intentionally circumvent the Federal Records Act. We found that the EPA implemented policies and procedures for preserving text messages, and took steps to make employees aware of the updated records management policy. However, management attention is still needed for the EPA's records management and Freedom of Information Act practices. Additionally, the EPA's mobile device management processes do not prevent employees from changing a device's configuration settings for retaining text messages on all government-issued mobile devices. We made six recommendations. The EPA indicated it completed corrective actions for two of the six recommendations and will implement the remaining four corrective actions by September 30, 2018.

- **Report No. [17-P-0029](#), *Acquisition Certifications Needed for Managers Overseeing Development of EPA's Electronic Manifest System*, dated November 7, 2016.** We reported that program and project managers responsible for overseeing development of the Electronic Manifest system did not obtain the required federal certification necessary to oversee a major acquisition. The EPA's February 2009 interim policy was outdated and did not reflect the December 2013 revisions made to the Federal Acquisition Certification for Program and Project Managers by the Office of Management and Budget. The EPA agreed with our two recommendations. The agency indicated that it completed corrective actions for the recommendations as of February 22, 2017.

## ***Distribution***

The Administrator  
Chief of Staff  
Chief of Staff for Operations  
Deputy Chief of Staff for Operations  
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 and Deputy Chief Information Officer,  
Office of Environmental Information  
Chief Information Security Officer, Office of Environmental Information  
Director, Office of Information Technology Operations, Office of Environmental Information  
Audit Follow-Up Coordinator, Office of the Administrator  
Audit Follow-Up Coordinator, Office of Environmental Information