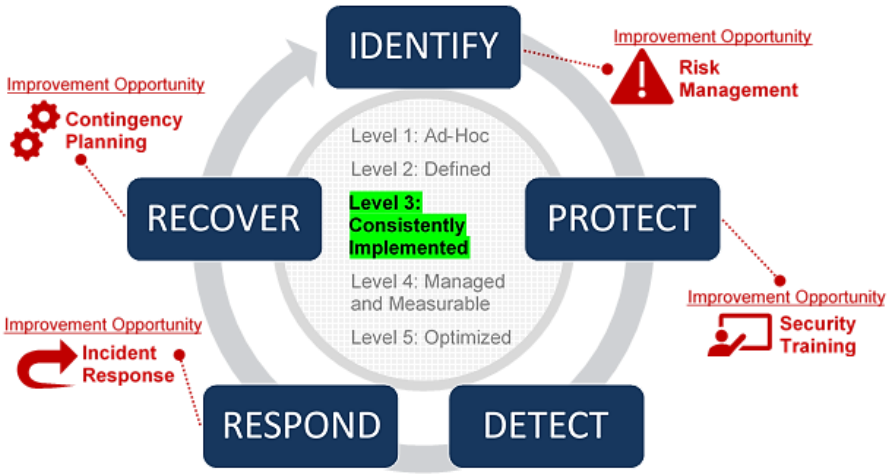
U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Compliance with the law
Operating efficiently and effectively

EPA Consistently Implements Processes Within Its Information Security Program, but Opportunities for Improvement Exist

Report No. 19-P-0058 **January 30, 2019**



Report Contributors:

Rudolph M. Brevard
Vincent Campbell
Nancy Dao
Eric Jackson Jr.
Gina Ross
Scott Sammons

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: Assessment of the EPA's information security program and opportunities for improvement. (EPA OIG image)

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

19-P-0058
January 30, 2019

At a Glance

Why We Did This Project

We 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) 2018.

The *Inspector General (IG) FISMA Reporting Metrics* document outlines five maturity levels for IGs to rate their agency's information security program:

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

We reported our audit results to the Office of Management and Budget (OMB). The OMB then calculates the overall maturity model level for each cybersecurity function within an agency's information security program.

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.

Listing of OIG reports.

EPA Consistently Implements Processes Within Its Information Security Program, but Opportunities for Improvement Exist

What We Found

The EPA has established an effective information security program for the five security functions and related domains defined in the *FY 2018 IG FISMA Reporting Metrics* and shown in the table below.

Further improvements are needed to strengthen internal processes to better protect human health and environmental data from cybersecurity threats.

Security functions	Domains
Identify	Risk management
Protect	Configuration management, identity and access management, data protection and privacy, and security training
Detect	Information security continuous monitoring
Respond	Incident response
Recover	Contingency planning

Source: *FY 2018 IG FISMA Reporting Metrics*.

We concluded that the EPA has achieved an overall assessment of Maturity Level 3, which denotes that the agency consistently implements its policies, procedures and strategies within its information security program. However, the EPA can further improve its processes in the following domains to strengthen its information security posture:

- **Risk Management**—Implement standard data elements for hardware assets connected to the network and for software and associated licenses used within the agency's environment.
- **Security Training**—Implement a process for reporting on contractors' completion of role-based training.
- **Incident Response**—Implement certain technologies to support the incident response program.
- **Contingency Planning**—Implement a process to ensure that the results of business impact analyses are used to guide contingency planning efforts.

Appendix A contains the results of our assessments for the *FY 2018 IG FISMA Reporting Metrics*. We worked closely with EPA officials and, where appropriate, revised our assessments. We briefed the EPA on the results of our analyses. We made no recommendations based on our analyses, and the EPA agreed with our conclusions.

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

OFFICE OF
INSPECTOR GENERAL

January 30, 2019

MEMORANDUM

SUBJECT: EPA Consistently Implements Processes Within Its Information Security Program, but Opportunities for Improvement Exist
Report No. 19-P-0058

FROM: Charles J. Sheehan, Acting Inspector General

TO: Donna J. Vizian, Principal Deputy Assistant Administrator
Office of Mission Support

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&E-FY18-0194. 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 the 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 primary oversight for the areas evaluated in this report is the Office of Information Security and Privacy within the Office of Mission Support.

You are not required to provide respond to this report because this report contains no recommendations. However, if you submit a response, it will be posted on the OIG's website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal along with corresponding justification.

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

Table of Contents

Appendices

Purpose

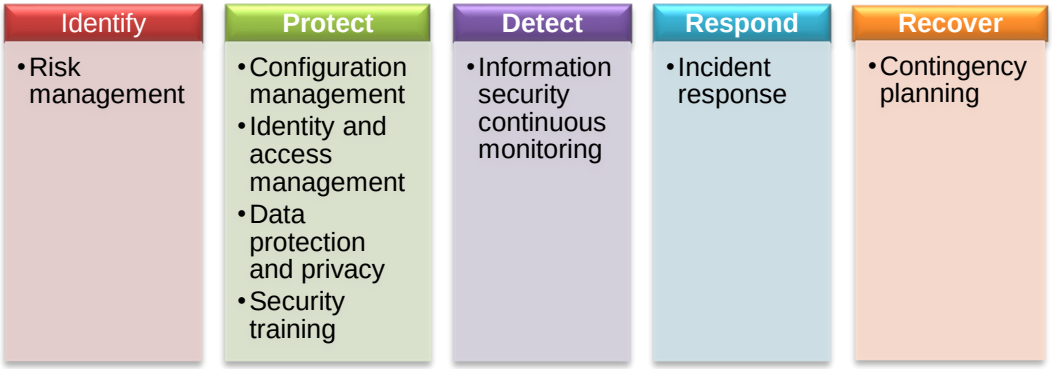
The U.S. Environmental Protection Agency (EPA), Office of Inspector General (OIG), conducted this audit to evaluate the EPA's compliance with the Federal Information Security Modernization Act of 2014 (FISMA) during fiscal year (FY) 2018.

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 2018 Inspector General (IG) FISMA Reporting Metrics* lists eight domains within the five security functions defined in the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Figure 1). Each security function contains at least one corresponding domain of an agency's information security program. This cybersecurity framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise.

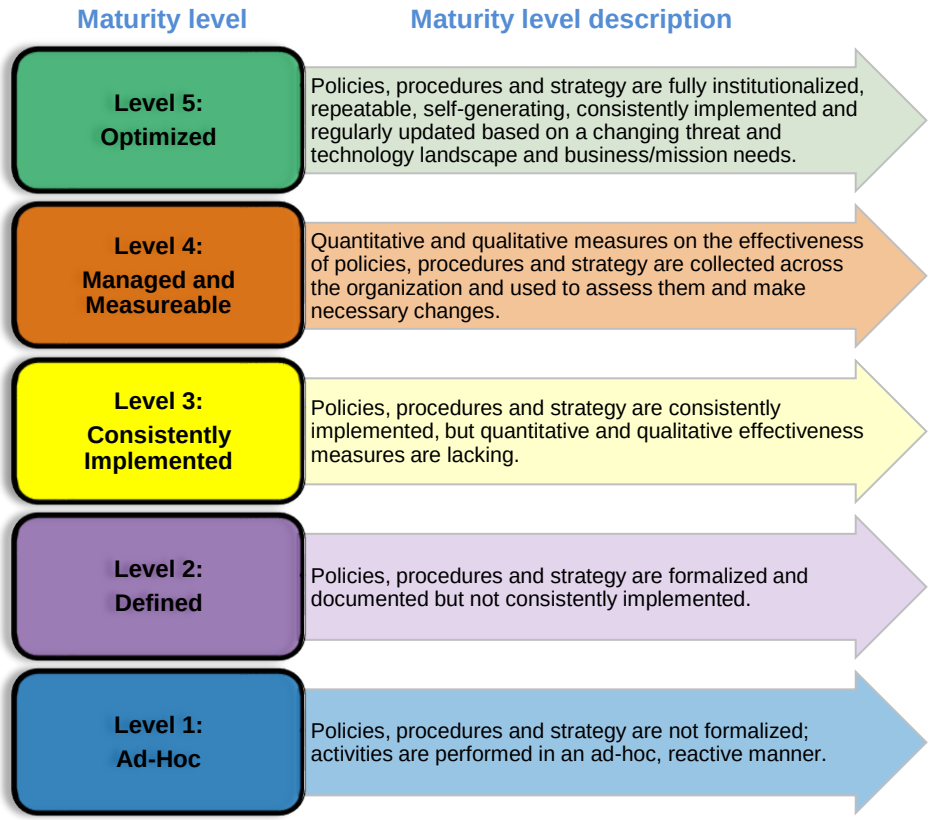
Figure 1: FY 2018 cybersecurity framework functions and domains



Source: *FY 2018 IG FISMA Reporting Metrics.*

The IG of each federal agency is required to assess the effectiveness of the agency's information security program on a maturity model spectrum, which is shown in Figure 2. The foundational levels of this five-tiered spectrum ensure that agencies develop sound policies and procedures (Levels 1 and 2), while the advanced levels capture the extent to which agencies institutionalize those policies and procedures (Levels 3, 4 and 5). Level 5, "Optimized," is the highest maturity level that an organization can achieve.

Figure 2: Maturity model levels



Source: *FY 2018 IG FISMA Reporting Metrics.*

To calculate the maturity level of a federal agency, the agency's IG assesses ratings for each of the eight domains shown in Figure 1. These ratings are produced by a simple majority, where the most frequent rating (i.e., the mode) across the metrics within each domain serves as the overall domain rating.[1] IGs are to submit the completed metrics for each domain to the Department of Homeland Security's CyberScope application.[2] Based on the completed metrics, the application will calculate an overall maturity model level based on a simple majority of the most frequent maturity level assessed for each cybersecurity framework function.

The reporting metrics indicate that maturity model Level 4, "Managed and Measurable," represents an effective level of security for an information security program. However, the reporting metrics provide IGs the discretion to rate an agency's information security program effective at a maturity level lower than Level 4.

[1] The domains and metrics to be evaluated each year are provided in an annual *IG FISMA Reporting Metrics* document. The FY 2018 reporting metrics are outlined in the *FY 2018 IG FISMA Reporting Metrics*, Version 1.0.1, issued May 24, 2018.
[2] Appendix A includes the EPA OIG's completed metrics submitted to the CyberScope application.

Responsible Office

The Office of Mission Support 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 Mission Support, the EPA's Chief Information Security Officer, who resides in the Office of Information Security and Privacy, 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 2018 to October 2018 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 tested whether the EPA defined and implemented the policies and procedures outlined within the *FY 2018 IG FISMA Reporting Metrics* for all FISMA domains, except the "data protection and privacy" domain. For this domain, we tested whether the agency developed the respective policies and procedures. However, we did not test the implementation, because the domain was newly added to the *FY 2018 IG FISMA Reporting Metrics*.

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 functions and domains. We judgmentally selected a sample of EPA and contractor systems to evaluate those FISMA metrics that require testing at the system level. Additionally, we selected samples of items for other FISMA domains, as appropriate, to assess some of the FISMA metrics. We also reviewed FY 2018 audit reports issued by the U.S. Government Accountability Office and the EPA OIG (Appendix B) to identify any issues related to the cybersecurity functions and domains.

Results

The EPA has an effective information security program. Using the *FY 2018 IG FISMA Reporting Metrics*, Version 1.0.1, dated May 24, 2018, we concluded that the EPA achieved an overall maturity level assessment of Level 3, "Consistently Implemented." This rating denotes that the agency consistently implements its information security program's policies and procedures.

However, further improvements are needed within the EPA's information security program. We concluded that the EPA did not consistently implement its policies and procedures for several FISMA metrics at Maturity Level 3 (Table 1).[3]

Table 1: EPA FISMA metrics assessed below Maturity Level 3

Security function	Security domain	FISMA metric
Identify	**Risk management**	• To what extent does the organization use standard data elements 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? • To what extent does the organization use standard data elements 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? • To what extent has the organization ensured that plans of action and milestones are utilized for effectively mitigating security weaknesses? • To what extent does the organization ensure that specific contracting language and service level agreements are included in appropriate contracts to mitigate and monitor risks related to contractor systems and services?
Protect	**Security training**	• To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities?
Respond	**Incident response**	• 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? • To what degree does the organization utilize certain technologies to support its incident response program?
Recover	**Contingency planning**	• To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts?

Source: OIG test results.

We worked closely with agency representatives and briefed them on each portion of the *FY 2018 IG FISMA Reporting Metrics* as the results were completed. We collected management's feedback on our analyses, analyzed additional documentation as needed and, as appropriate, updated our assessments. Management agreed with our conclusions. Appendix A contains the detailed results of our analyses.

[3] The "data protection and privacy" domain assessment is excluded from Table 1 because this domain is a new area added to the *FY 2018 IG FISMA Reporting Metrics*. We concluded that the EPA has achieved Maturity Level 2, "Defined," in this area, which denotes that the agency has developed policies and procedures for its privacy program.

Conclusion

While the EPA demonstrated that it has implemented an information security program consistent with the majority of the FISMA metrics, management needs to improve business processes in select domains. These improvements would establish the agency as a high-performing organization in protecting the availability and integrity of environmental data from loss, alteration and destruction. This protection is essential to advancing the protection of human health and the environment.

Appendix A

OIG-Completed CyberScope Template for EPA's Information Security Program

Inspector General
Section Report

2018
Annual FISMA Report

Environmental Protection Agency

Function 1: Identify - Risk Management

1 To what extent 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, PM-5, and CM-8; OMB M-04-25; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2018 CIO FISMA Metrics: 1.1, 1.4, and 1.5)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 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; FY 2018 CIO FISMA Metrics: 1.2)?

Defined (Level 2)

Comments: The EPA has not implemented standard data elements\taxonomy for hardware assets connected to the agency's network.

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: The EPA has not implemented standard data elements\taxonomy for software and associated licenses used within its' environment.

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; FIPS 199; FY 2018 CIO FISMA Metrics: 1.1)?

Consistently Implemented (Level 3)

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that includes 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 SP 800-39; NIST SP 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; FY 2018 CIO FISMA Metrics: 1.6)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 13.2.

Function 1: Identify - Risk Management

6 To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (NIST SP 800-39; FEA Framework; NIST SP 800-53: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; DHS Binding Operational Directive 17-01)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 13.2.

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, 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 SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2; OMB A-123; CFO Council ERM Playbook)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 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: EPA personnel did create POA&Ms within the agency's specified timeframes for known security weaknesses.

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) security controls to mitigate system-level risks (NIST SP 800-37; NIST SP 800-39; NIST SP 800-53: PL-2 and RA-1; NIST SP 800-30; CSF:ID.RA-1 – 6)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 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; OMB Circular A-11; Green Book (Principles #9, #14 and #15))?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 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, and 52.239-1; President's Management Council; NIST SP 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2018 CIO FISMA Metrics: 1.5; Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)?

Defined (Level 2)

Comments: EPA personnel did not include agency-specified information security clauses in new procurements as required by the EPA's directive.

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)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 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 in FISMA metric 13.2.

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?

We did not conduct any testing beyond maturity level 3 (Consistently Implemented). Based on our review of the EPA's processes and supporting documentation, we conclude that the EPA has an effective risk management program.

Calculated Maturity Level - Consistently Implemented (Level 3)

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; NIST SP 800-128: Section 2.4)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 22.

Function 2A: Protect - Configuration Management

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 phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53: CM-9)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 22.

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 SP 800-128: 2.2.1)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 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 and CM-8; FY 2018 CIO FISMA Metrics: 1.1 and 2.2; CSF: ID.DE.CM-7)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 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 2018 CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 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 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20, Control 4.5; FY 2018 CIO FISMA Metrics: 2.13; and DHS Binding Operational Directive 15-01)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 22.

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-08-05)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 22.

Function 2A: Protect - Configuration Management

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 SP 800-53: CM-2 and CM-3)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 22.

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?

We did not conduct any testing beyond maturity level 3 (Consistently Implemented). Based on our review of the EPA's processes and supporting documentation, we conclude that the EPA has an effective configuration management program.

Calculated Maturity Level - Consistently Implemented (Level 3)

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 SP 800-53: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Consistently Implemented (Level 3)

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

Consistently Implemented (Level 3)

Comments: See comment in FISMA Metric 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 26 through 31) (NIST SP 800-53: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; FY 2018 CIO FISMA Metrics: 2.3).

Consistently Implemented (Level 3)

Comments: See comment in FISMA Metric 32.

Function 2B: Protect - Identity and Access Management

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 and PS-3; National Insider Threat Policy; FY 2018 CIO FISMA Metrics: 2.16)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA Metric 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)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA Metric 32.

28 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 Identity Assurance Level (IAL)3/ Authenticator Assurance Level (AAL) 3/ Federated Assurance Level (FAL) 3 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; FY 2018 CIO FISMA Metrics: 2.4; and Cybersecurity Sprint)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA Metric 32.

29 To what extent has the organization implemented strong authentication mechanisms (two-factor PIV credential or other NIST 800-63 r3 IAL 3/ AAL 3/ FAL 3 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; FY 2018 CIO FISMA Metrics: 2.5; and Cybersecurity Sprint)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA Metric 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 2018 CIO FISMA Metrics: 2.4 and 2.5; NIST SP 800-53: AC-1, AC-2 (2), and AC-17; CSIP)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA Metric 32.

Function 2B: Protect - Identity and Access Management

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 and SI-4; and FY 2018 CIO FISMA Metrics: 2.10)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA Metric 32.

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?

We did not conduct any testing beyond maturity level 3 (Consistently Implemented). Based on our review of the EPA's processes and supporting documentation, we conclude that the EPA has an effective identity and access management program.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2C: Protect - Data Protection and Privacy

33 To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; OMB M-18-02; OMB A-130, Appendix I; NIST SP 800-53: AR-4 and Appendix J)?

Defined (Level 2)

Comments: See comment in FISMA metric 38.

34 To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (NIST SP 800-53; Appendix J, SC-8, SC-28, MP-3, and MP-6; FY 2018 CIO FISMA Metrics: 2.9 and 2.10)?

Encryption of data at rest
Encryption of data in transit
Limitation of transfer to removable media
Sanitization of digital media prior to disposal or reuse

Defined (Level 2)

Comments: See comment in FISMA metric 38.

Function 2C: Protect - Data Protection and Privacy

35 To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2018 CIO FISMA Metrics: 3.8 – 3.12)?

Defined (Level 2)

Comments: See comment in FISMA metric 38.

36 To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17-25)?

Defined (Level 2)

Comments: See comment in FISMA metric 38.

37 To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53: AR-5)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)?

Defined (Level 2)

Comments: See comment in FISMA metric 38.

38 Provide any additional information on the effectiveness (positive or negative) of the organization's data protection and privacy 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 data protection and privacy program effective?

We did not conduct any testing beyond maturity level 2 (Defined). Based on our review of the EPA's policies and procedures, we conclude that the EPA has an effective data protection and privacy program.

Calculated Maturity Level - Defined (Level 2)

Function 2D: Protect - Security Training

39 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 SP 800-53: AT-1; and NIST SP 800-50).

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 45.2.

Function 2D: Protect - Security Training

40 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 SP 800-53: AT-2 and AT-3; NIST SP 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS/SANS Top 20: 17.1)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 45.2.

41 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 SP 800-53: AT-1; NIST SP 800-50: Section 3).

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 45.2.

42 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 of questions 43 and 44 below) (NIST SP 800-53: AT-1 through AT-4; and NIST SP 800-50).

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 45.2.

43 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 SP 800-53: AT-2; FY 2018 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; SANS Top 20: 17.4).

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 45.2.

Function 2D: Protect - Security Training

44 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 SP 800-53: AT-3 and AT-4; FY 2018 CIO FISMA Metrics: 2.15)?

Defined (Level 2)

Comments: The EPA has developed a process for reporting contractors' completion status of role-based training; however, the process will not be fully implemented until Fiscal Year 2019.

45.1 Please provide the assessed maturity level for the agency's Protect Function.

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 45.2.

45.2 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?

We did not conduct any testing beyond maturity level 3 (Consistently Implemented). Based on our review of the EPA's processes and supporting documentation, we conclude that the EPA has an effective security training program.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 3: Detect - ISCM

46 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)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 51.2.

47 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; collection of 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 49)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 51.2.

Function 3: Detect - ISCM

48 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 2018 CIO FISMA Metrics)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 51.2.

49 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)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 51.2.

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

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 51.2.

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

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 51.2.

51.2 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?

We did not conduct any testing beyond maturity level 3 (Consistently Implemented). Based on our review of the EPA's processes and supporting documentation, we conclude that the EPA has an effective information security continuous monitoring program.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 4: Respond - Incident Response

52 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 SP 800-61 Rev. 2; NIST SP 800-184; OMB M-17-25; OMB M-17-09; FY 2018 CIO FISMA Metrics: 4.1, 4.3, 4.6, and 5.3; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 59.2.

Function 4: Respond - Incident Response

53 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: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2018 CIO FISMA Metrics: Section 4; and US-CERT Federal Incident Notification Guidelines)?

Defined (Level 2)

Comments: The EPA's enterprise incident response capabilities lack adequate resources and do not have integrated incident response processes.

54 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; OMB M-18-02; and US-CERT Incident Response Guidelines)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 59.2.

55 How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 59.2.

56 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-18-02; NIST SP 800-53: IR-6; US-CERT Incident Notification Guidelines; PPD-41; DHS Cyber Incident Reporting Unified Message)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 59.2.

57 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, including through contracts/agreements, as appropriate, for incident response support (FY 2018 CIO FISMA Metrics: 4.4; NIST SP 800-86; NIST SP 800-53: IR-4; OMB M-18-02; PPD-41).

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 59.2.

Function 4: Respond - Incident Response

58 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; NIST SP 800-44)

Defined (Level 2)

Comments: The EPA has not implemented certain technologies.

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

Consistently Implemented (Level 3)

Comments: See comment in FISMA Metric 59.2.

59.2 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?

We did not conduct any testing beyond maturity level 3 (Consistently Implemented). Based on our review of the EPA's processes and supporting documentation, we conclude that the EPA has an effective incident response program.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 5: Recover - Contingency Planning

60 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 SP 800-53: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 67.2.

Function 5: Recover - Contingency Planning

61 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 62-66) (NIST SP 800-34; NIST SP 800-161; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5).

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 67.2.

62 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17-09; FY 2018 CIO FISMA Metrics: 5.6)?

Defined (Level 2)

Comments: The EPA did not have a current business impact assessment for its' National Hosting System.

63 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800-53: CP-2; NIST SP 800-34; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 67.2.

64 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53: CP-3 and CP-4; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 67.2.

65 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2018 CIO FISMA Metrics: 5.4; and NARA guidance on information systems security records)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 67.2.

66 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 SP 800-53: CP-2 and IR-4)?

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 67.2.

Function 5: Recover - Contingency Planning

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

Consistently Implemented (Level 3)

Comments: See comment in FISMA metric 67.2.

67.2 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?

We did not conduct any testing beyond maturity level 3 (Consistently Implemented). Based on our review of the EPA's processes and supporting documentation, we conclude that the EPA has an effective contingency planning program.

Calculated Maturity Level - Consistently Implemented (Level 3)

Comments: EPA information security program considered effective at maturity level 3 (Consistently Implemented)

Function 0: Overall

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

Effective

Function 0: Overall

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.

The Data Protection and Privacy Domain was a new area added to the FY2018 Inspector General (IG) Federal Information Security Modernization Act (FISMA) Reporting Metrics and we concluded that the EPA had developed policies, procedures and strategies to manage the agency's privacy program. For the remaining cybersecurity functions and domains, we concluded that the EPA has processes to consistently implement its policies, procedures and strategies to meet the requirements of the cybersecurity functions and related domains outlined in the FY2018 IG FISMA reporting metrics.

We did identify some areas within the EPA's information security program that lacked evidence for us to conclude that the processes have been consistently implemented; as such, we assessed those FISMA metrics at the respective maturity level based on our analyses. Those areas are located in:

Risk Management
Security Training
Incident Response
Contingency

Overall, we concluded that the EPA has reached maturity Level 3 (Consistently Implemented) within the IG's FISMA maturity model for those elements of the FISMA metrics we tested.

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	0
Defined	4
Consistently Implemented	8
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	8
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	9
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 2C: Protect - Data Protection and Privacy

Function	Count
Ad-Hoc	0
Defined	5
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)Not Effective	0

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	6
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)Not Effective	0

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See comment in FISMA metric 13.2.
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See comment in FISMA metric 45.2.
Function 3: Detect - ISCM	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See comment in FISMA metric 51.2.
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See comment in FISMA Metric 59.2.
Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See comment in FISMA metric 67.2.
Overall	Not Effective	Effective	EPA information security program considered effective at maturity level 3 (Consistently Implemented)

Appendix B

Information Security Reports Issued in FY 2018

The EPA OIG issued the following reports in FY 2018 that included recommendations regarding improvements within the EPA's information security program:

Report No. **18-P-0217**, *Management Alert: To Minimize Risk of Environmental Harm, the Security Categorization of Electronic Manifest System Data Needs to Be Re-Evaluated*, June 21, 2018. We reported that the EPA categorized the sensitivity of the information in its Electronic Manifest (e-Manifest) system at such a low level that planned information system security controls would not minimize the risk of environmental harm. This occurred because the EPA (1) did not sufficiently consider homeland security implications as they relate to chemicals of interest, (2) considered the e-Manifest information to be in a low-risk category that only requires minimal system security controls to be implemented for protection, and (3) did not consider further uses of the e-Manifest system (e.g., the system could potentially be used by first responders in efforts to remediate incidents involving the transportation of hazardous waste). A breach of hazardous material information may facilitate terrorist or other criminal activities. We made three recommendations, and the EPA agreed with each recommendation. The EPA will provide planned correction actions in response to the report's recommendations.

Report No. **18-P-0234**, *Without a Process for Monitoring Sensitive Data, EPA Region 4 Risks Unauthorized Access to File Servers and Share Folders,* August 28, 2018. We determined that a share folder found on EPA Region 4 file servers did not comply with federal and agency guidance for access administration. The Region 4 share folder contained sensitive data, and the region did not have a process to monitor user activity or content in file servers' share folders. Federal and agency guidance requires agencies to implement security controls for their information systems and related components. Information system components include file servers and the share folders they host. Region 4 lacked documented procedures for EPA information technology security control requirements applicable to file servers and share folders. In addition, Region 4 lacked documented procedures for monitoring share folder access or content. EPA data were vulnerable to unauthorized access because Region 4 did not create procedures to ensure that EPA security control requirements were implemented for file servers and share folders. The lack of procedures, combined with the lack of audit logging or an audit log review process, put the EPA at risk for unauthorized activity being undetected and uninvestigated. Sensitive data are vulnerable to unauthorized disclosure without a tool or process in place to monitor user activity and access to share folders found on EPA Region 4 file servers. Region 4 agreed with our report and recommendation. The region completed all proposed corrective actions by August 14, 2018, and those actions satisfy the intent of the recommendation.

Report No.**18-P-0298**, *Management Alert: EPA's Incident Tracking System Lacks Required Controls to Protect Personal Information,* September 28, 2018. The EPA's incident tracking system lacked the required security controls to (1) protect the confidentiality of personally

identifiable information (PII) and sensitive personally identifiable information (SPII) and (2) enforce password management requirements, even though the requirements are specified in federal and agency guidance. The EPA was unaware that PII and SPII were included on incident tickets handled by help desk technicians and retained in the incident tracking system where they can be viewed by all registered users (EPA employees and contractors). We found that current operating procedures do not instruct help desk technicians to exclude PII and SPII within incident tickets or to follow the EPA's information security and privacy directives to protect the confidentiality of PII and SPII. As a result, we identified 25 incident tickets within the agency's incident tracking system that disclosed Social Security numbers, W-2 information, dates of birth, home addresses and Thrift Savings Plan account information. The EPA began a partial rollout of a replacement incident tracking system in May 2018. The rollout had an anticipated completion date of September 30, 2018. Therefore, we issued this report to reiterate the need for management to address current weaknesses, so that the weaknesses do not continue to impair the EPA's ability to protect the confidentiality of PII and SPII. The lack of required privacy and security controls to protect PII and SPII could lead to identity theft. The agency agreed with two of the four recommendations, and we consider those recommendations resolved with corrective actions pending. The remaining two recommendations are unresolved.

Appendix C

Distribution

The Administrator
Deputy Administrator
Chief of Staff
Chief of Operations
Special Advisor, Office of the Administrator
Assistant Administrator for Mission Support
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Principal Deputy Assistant Administrator for Mission Support
Director, Information Security and Management Staff, Office of Mission Support
Deputy Assistant Administrator for Environmental Information and Chief Information Officer, Office of Mission Support
Director, Office of Continuous Improvement, Office of the Administrator
Director and Chief Information Security Officer, Office of Information Security and Privacy, Office of Mission Support
Director, Office of Information Technology Operations, Office of Mission Support
Director, Office of Resources and Business Operations, Office of Mission Support
Audit Follow-Up Coordinator, Office of the Administrator
Audit Follow-Up Coordinator, Office of Mission Support